

Cisco IOS Cookbook
中文精简版

V1.5 版

原著 Kevin Dooley 和 Ian J. Brown

翻译 NeoShi



前言

Cookbook 书系算是 OReilly 的一个出版品牌，这套丛书的特点就是可以帮助你快速找到解决问题的方法，而不需要你从大量的文档中去查找，你可以现学现卖，就像菜谱一样，照着里面的步骤去做就行了，当然也要注意下里面的参考注释。这本 Cisco IOS Cookbook 就是专注于思科 IOS 系统配置的，可以当做一本应急手册来使用，也可以逐篇阅读，因为里面很多小技巧也许你从来没有注意过。这本书是第二版，跟前一版相比有什么区别呢，很明显的就是书名变了，从 Cisco Cookbook 变为 Cisco IOS Cookbook，这样让书名更名副其实，毕竟思科现在的产品线很长，以后也许有 Cisco PIX Cookbook 之类的。在内容上更新在于涵盖了 IOS 12.4 的新特性，当然原有的内容还继续保留，毕竟思科的很多配置向后兼容，只是特别注明了一些新选项而已，同时与时俱进增加了四个新的章节：IP Mobility, IP Version 6, MPLS, 和 Security，这样就更符合现在的趋势。

这本中文精简版每章的内容基本和原版保持一致，可能会省掉部分脚本。文中格式按照提问，回答和注释三部分排列，注释部分不是对原版的全盘翻译，只是个人对配置的一些意见和注意事项，如果有什么错漏以原版为主。此次翻译从 2007 年 1 月 23 日开始，基本一天一章在我的 Blog 发帖，持续了两个月，很感谢一直跟我在一起的 QQ 群里的朋友：绿豆大叔，``，猴哥，偶像 miFor，财神 Monk，帅哥 Alex，兔总，若然等（谁也别吵吵，排名不分先后反正☺），也感谢一直关注我 Blog 的不知名朋友们。

英文原版下载：http://dreamz.org/Files/neoshi/OReilly.Cisco.IOS.Cookbook.2nd.Edition.Dec.2006.rar

本书的 Google Group：http://groups.google.com/group/ios-cookbook

联系 Email： ioscookbook@neoshi.net 或者 neoshi@gmail.com

NeoShi

有福之州

2007-3-27

目录

第一章 路由器配置和文件管理

1.1. 通过 TFTP 来配置路由器

提问 使用 TFTP 来加载路由器的配置文件

回答

Router1#**copy tftp://*172.25.1.1/NEWCONFIG* running-config**

Destination filename [running-config]? **<enter>**

Accessing tftp://172.25.1.1/NEWCONFIG...

Loading NEWCONFIG from 172.25.1.1 (via FastEthernet0/0.1): !

[OK - 24 bytes]

24 bytes copied in 0.192 secs (125 bytes/sec)

Router1#

注释 IOS12.0 版本以前使用 **configure network** 命令，另外拷贝至路由器的配置文件应该以 End 结尾，否则会出现下面的错误提示信息：%PARSER-4-BADCFG: Unexpected end of configuration file.

1.2. 保存路由器配置到服务器

提问 保存路由器当前配置文件到 TFTP 服务器作为备份

回答

Freebsd% **touch */tftpboot/router1-confg***

Freebsd% **chmod 666 */tftpboot/router1-confg***

Freebsd% **telnet *Router1***

Trying 172.25.1.5...

Connected to Router1.

Escape character is '^]'.

User Access Verification

Password: ***<vtypassword>***

Router1>**enable**

Password: ***<enablepassword>***

Router1#**copy running-config tftp://*172.25.1.1/router1-confg***

Address or name of remote host [172.25.1.1]? **<enter>**

Destination filename [router1-confg]? **<enter>**

!!!

9640 bytes copied in 3.956 secs (2437 bytes/sec)

Router1#

注释 确保 TFTP 服务器上的目录和文件可写

1.3. 使用远端配置文件启动路由器

提问 使用另外的配置文件来启动路由器

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**service config**

Router1(config)#**boot network tftp *Network-auto 172.25.1.1***

Router1(config)#**boot host tftp *Router8-auto 172.25.1.1***

Router1(config)#**end**

Router1#

注释 **service config** 缺省是关闭的，如果打开后缺省会去查找的文件名为 network-config, cisconet.cfg, router1-confg, router1.cfg 等

1.4. 保存大于 NVRAM 大小的配置文件

提问 配置文件过大，超过了可用的 NVRAM 大小

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**service compress-config**

Router1(config)#**end**

Router1#

注释 可以使用 show startup-config 来验证

Router1#**show startup-config**

Using 5068 out of 29688 bytes, uncompressed size = 9969 bytes

Uncompressed configuration from 5068 bytes to 9969 bytes

1.5. 清除启动配置文件

提问 清除配置文件恢复到出厂设置

回答

Router1#**erase nvram:** （**erase startup-config**）

Erasing the nvram filesystem will remove all files! Continue? [confirm] <enter>

[OK]

Erase of nvram: complete

Router1#**reload**

System configuration has been modified. Save? [yes/no]: **no**

Proceed with reload? [confirm] **<enter>**

注释 无

1.6. 加载新的 IOS 镜像

提问 升级当前的 IOS

回答

Router1#**copy tftp://*172.25.1.1/c2600-ik9o3s-mz.122-12a.bin flash:***

Destination filename [c2600-ik9o3s-mz.122-12a.bin]? ***<enter>***

Accessing tftp://172.25.1.1/c2600-ik9o3s-mz.122-12a.bin...

Erase flash: before copying? [confirm] ***<enter>***

Erasing the flash filesystem will remove all files! Continue? [confirm] ***<enter>***

Erasing device... eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee ...erased

Erase of flash: complete

Loading c2600-ik9o3s-mz.122-12a.bin from 172.25.1.1 (via FastEthernet0/0.1):!!!!!!!!!!!!!!

[OK - 11135588 bytes]

Verifying checksum... OK (0xE643)

11135588 bytes copied in 82.236 secs (135410 bytes/sec)

Router1# ***reload***

Proceed with reload? [confirm] ***<enter>***

注释 无

1.7. 以另一个 IOS 镜像文件启动

提问 使用其它的 IOS 镜像启动

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**boot system *flash:c3620-jk9o3s-mz.122-7a.bin***

Router1(config)#**boot system *flash:c3620-jos56i-l.120-11.bin***

Router1(config)#**boot system *slot0:c3620-ik9s-mz.122-13.bin***

Router1(config)#**boot system rom**

Router1(config)#**end**

注释 boot system 命令的顺序非常重要，如果使用新的 IOS，建议先进行 no boot system 的操作。从 IOS 12.3(4)T 后思科引入了 boot markers 的概念，所有的 boot systme 命令都会放在 boot markers 之间，比如：

Router1#**show running-config | include ^boot**

boot-start-marker

boot system slot0:c3745-ipbasek9-mz.124-6.T.bin

boot system slot0:c3745-ipbasek9-mz.124-7.bin

boot system flash:

boot-end-marker

Router1#

1.8. 通过网络启动

提问 IOS 太大本地 Flash 无法保存，使用保存在网络上的 IOS 启动

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**boot system tftp *c2500-io-l.122-7a.bin 172.25.1.1***

Router1(config)#**boot system flash**

Router1(config)#**end**

Router1#

注释 无

1.9. 拷贝 IOS 镜像文件到服务器

提问 保存一份 IOS 到 TFTP 服务器作为备份

回答

Freebsd% **touch */tftpboot/c2600-ik9o3s-mz.122-12a.bin***

Freebsd% **chmod 666 */tftpboot/c2600-ik9o3s-mz.122-12a.bin***

Freebsd% **telnet *Router1***

Trying 172.25.1.5...

Connected to Router1.

Escape character is '^]'.

User Access Verification

Password: **<vtypassword>**

Router1>**enable**

Password: **<enablepassword>**

Router1#**copy flash:*c2600-ik9o3s-mz.122-12a.bin* tftp**

Address or name of remote host []? ***172.25.1.1***

Destination filename [c2600-ik9o3s-mz.122-12a.bin]? **<enter>**

!!!!!!

11135588 bytes copied in 52.588 secs (211752 bytes/sec)

Router1#

注释 无

1.10. 通过控制台口拷贝 IOS 镜像文件

提问 通过控制台口和 AUX 端口来加载 IOS

回答

Router1#**copy xmodem: slot1:**

**** WARNING ****

x/ymodem is a slow transfer protocol limited to the current speed

settings of the auxiliary/console ports. The use of the auxilary

port for this download is strongly recommended.

During the course of the download no exec input/output will be

available.

---- ******* ----

Proceed? [confirm] **<enter>**

Destination filename []? ***c3620-ik9s-mz.122-12a.bin***

Erase slot1: before copying? [confirm] **<enter>**

Use crc block checksumming? [confirm] **<enter>**

Max Retry Count [10]: **<enter>**

Perform image validation checks? [confirm] **<enter>**

Xmodem download using crc checksumming with image validation

Continue? [confirm] **<enter>**

Ready to receive file...........CC **<start xmodem file transfer here>**

4294967295 bytes copied in 1450.848 secs (1271445669961 bytes/sec)

Router1#

注释 思科建议使用 AUX 口进行此步骤，因为 AUX 口支持硬件流控。为了提高拷贝速度，建议提前使用下述命令来设置端口速度

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**line aux 0**

Router1(config-line)#**speed *115200***

Router1(config-line)#**end**

Router1#

1.11. 删除 FLASH 中的文件

提问 删除 Flash 中的文件

回答

Router1#**erase *slot1:***

Erasing the slot1 filesystem will remove all files! Continue? [confirm] **<enter>**

Erasing device... eeeeeeeeeeee ...erased

Erase of slot1: complete

Router1#

或者删除单个文件

Router1#**delete *slot1:c3620-ik9s-mz.122-13.bin***

Delete filename [c3620-ik9s-mz.122-13.bin]? **<enter>**

Delete slot1:c3620-ik9s-mz.122-13.bin? [confirm] **<enter>**

Router1#

注释 并不是所有的路由器都支持 erase 命令，不行的话可以尝试 format 命令，有些路由器在使用 delete 命令以后还可以使用 undelete 来恢复，同时也需要使用 squeeze 来彻底删除文件

1.12. 对 FLASH 进行分区

提问 对 Flash 进行分区

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**partition slot1: *2 8 8***

Router1(config)#**end**

Router1#

注释 如果 erase 不支持也可以试试 partition 命令

1.13. 配置路由器为 TFTP 服务器

提问 配置路由器为 TFTP 服务器

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**tftp-server *flash:c2600-ik9o3s-mz.122-12a.bin***

Router1(config)#**end**

Router1#

注释 使用此命令并不能把路由器配置为全功能的 TFTP 服务器，此服务器只能用于文件下载，而不能进行上传

1.14. 在路由器上使用 FTP

提问 在路由器上使用 FTP 来进行文件的下载

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip ftp username *neoshi***

Router1(config)#**ip ftp password *ioscookbook***

Router1(config)#**end**

Router1#**copy ftp: running-config**

Address or name of remote host [172.25.1.1]? ***172.25.1.1***

Source filename []? ***test***

Destination filename [running-config]? **<enter>**

Accessing ftp://172.25.1.1/test...

Loading /test

[OK - 24/4096 bytes]

24 bytes copied in 0.276 secs (87 bytes/sec)

Router1#

当然也可以使用下面的简化命令

copy *ftp://neoshi：ioscookbook@172.25.1.1/c3620-ik9s-mz.122-10a.bin slot1:*

注释 如果没有指定用户名和密码，路由器缺省会使用匿名登录

1.15. 批量产生路由器配置文件

1.16. 同时改变多台路由器的配置

1.17. 获的设备的硬件信息

1.18. 备份路由器的配置

以上都是使用 perl 脚本来进行批量化操作，建议使用我推荐的图形化绿色免费工具软件

1.19. 热重启

提问 重启路由器而对业务影响减少到最低

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**warm-reboot**

Router1(config)#**end**

Router1#

注释 要使用热启动必须先冷启动一次…无语了吧哈哈。此特性开始于 12.3（2）T，根据实验冷启动要比热启动慢 4 分钟。可以使用 reload warm 命令进行人工的热重启

1.20. 热升级

提问 升级路由器 IOS 而对业务影响最小

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**warm-reboot**

Router1(config)#**end**

Router1#**reload warm file *slot0:c3745-ipbasek9-mz.124-7.bin***

注释 12.3(11)T 开始支持此特性

1.21. 配置存档特性

提问 自动对路由器配置进行存档

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**archive**

Router1(config-archive)#**path *slot0:/configs/$h***

Router1(config-archive)#**write-memory**

Router1(config-archive)#**time-period *1440***

Router1(config-archive)#**end**

Router1#

注释 从 12.3(4)T 开始思科引入配置存档特性，每次使用 wr 对配置进行保存的时候都会在路由器上生成一个存档配置文件，当然也可以像示例那样每 1440 分钟保存一次，使用 show archive 命令来显

示当前的配置存档，缺省保存 14 个文件，并且提供了配置比较命令 show archive config differences slot0:/configs/Router1-1 更提供了配置回滚的命令 configure replace slot0:/configs/Router1-1 方便的回滚到以前的配置。对于保存的配置文件名可以$h 来代表设备主机名$t 来代表时间

1.22. 路由器配置锁定

提问 防止多个用户同时对路由器配置文件进行修改

回答

自动进行配置锁定

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**configuration mode exclusive auto**

Router1(config)#**end**

Router1#

按需进行配置锁定

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**configuration mode exclusive manual**

Router1(config)#**end**

Router1#

注释 12.3(14)T 引入了此特性防止多个用户同时对路由器配置进行修改，在配置为 auto 的模式下，如果有用户进入了配置模式就自动对配置进行锁定，在 manual 模式下可以使用 **configure terminal lock** 进行配置锁定，可以使用 **show configuration lock** 来查看当前的配置锁定信息，如果你确实需要进行配置，就把看到锁定的人踢掉吧。。

2.1. 创建命令别名

提问 为常用的命令创建简洁的别名

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**alias exec *rt* show ip route**

Router1(config)#**alias exec *on* show ip ospf neighbor**

Router1(config)#**end**

Router1#

注释 **show aliases** 命令可以输出当前配置的别名

2.2. 管理路由器 ARP 缓存

提问 修改 ARP 表条目超时时长

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface *Ethernet0***

Router1(config-if)#**arp timeout *600***

Router1(config-if)#**end**

Router1#

注释 缺省情况为 4 个小时，同时思科没有提供命令能单独的清除某个 ARP 缓存，只能通过 **clear arp** 命令来清除整个 ARP 表

2.3. 路由器 BUFFER 调整

提问 手动调整路由器 Buffer 分配来使其工作的更高效

回答

路由器维护两个 Buffer 池，public buffers 和 interface buffers

调整 public buffers

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**buffers big initial *100***

Router1(config)#**buffers big max-free *200***

Router1(config)#**buffers big min-free *50***

Router1(config)#**buffers big permanent *50***

Router1(config)#**end**

Router1#

调整 interface buffers

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**buffers *Ethernet0* initial *200***

Router1(config)#**buffers *Ethernet0* max-free *300***

Router1(config)#**buffers *Ethernet0* min-free *50***

Router1(config)#**buffers *Ethernet0* permanent *50***

Router1(config)#**end**

Router1#

注释 一般不建议修改，如果修改，建议首先使用 **show buffers** 命令来查看当前 buffer 使用情况，调整完以后建议使用 **show memory** 来查看内存使用情况

2.4. 自动调整路由器 BUFFER

提问 希望路由器根据自己的情况自动进行 buffer 分配调整

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#buffers tune automatic

Router(config)#**end**

Router#

注释 此命令引自 IOS 12.3(14)T，使用 **show buffers tune** 命令来查看自动调整情况

2.5. 使用 CDP 协议

提问 希望获的相连网络设备的信息

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**cdp run**

Router1(config)#**interface *Serial0/0***

Router1(config-if)#**cdp enable**

Router1(config-if)#**exit**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**no cdp enable**

Router1(config-if)#**exit**

Router1(config)#**interface *FastEthernet1/0***

Router1(config-if)#**cdp enable**

Router1(config-if)#**end**

Router1#

注释 CDP(Cisco Discovery Protocol)是思科专有的协议，用于发现相连的思科设备，帮助了解网络拓朴，缺省是启用的，使用 **show cdp neighbor detail** 命令可以查看相连设备的详细信息

2.6. 禁止 CDP 协议

提问 为了安全原因不想让邻近设备发现自己设备的信息

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**cdp run**

Router1(config)#**interface** FastEthernet0/0

Router1(config-if)#**no cdp enable**

Router1(config-if)#**end**

Router1#

注释 为了安全可以在边界设备上禁止 CDP

2.7. 小服务的开启

提问 开启或者禁用一些类似 finger 的小服务

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**service tcp-small-servers** （**no service tcp-small-servers**）

Router1(config)#**service udp-small-servers** **(no sercie udp-small-servers)**

Router1(config)#**end**

Router1#

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip finger** **(no ip finger)**

Router1#

注释 tcp 和 udp 的小服务指开启路由器的 echo,discard,daytime 和 chargen 服务，为了安全都建议将其关闭

2.8. 启用路由器 HTTP 访问

提问 通过浏览器来配置和管理路由器

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**access-list *75* permit *172.25.1.1***

Router1(config)#**access-list *75* deny any**

Router1(config)#**ip http server**

Router1(config)#**ip http access-class *75***

Router1(config)#**end**

Router1#

注释 由于 IOS 12.1(5)之前存在 HTTP 访问的高危漏洞，所以如果你的 IOS 版本小于此版本建议不要开启此服务

2.9. 启用路由器安全 HTTPS 访问

提问 通过加密的方式 HTTP 访问路由器

回答

Core#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Core(config)#**ip http secure-server**

Core(config)#**end**

Core#

注释 IOS 12.2(14)S 之后引入此特性，建议先用 **no ip http server** 命令关闭非加密的 HTTP 访问，然后开启安全的访问，同时可以使用 **ip http secure-port** *8080* 命令来更改访问端口

2.10. 使用静态主机名映射

提问 在路由器上配置静态的主机映射表，从而使用主机名而不是 IP 地址来访问设备

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip host *freebsd 172.25.1.1***

Router1(config)#**ip host *router2 10.1.1.1 172.22.1.4***

Router1(config)#**end**

Router1#

注释 可以对一个主机名映射很多 IP 地址来提供冗余访问，**show hosts** 命令来验证

2.11. 启用 DNS 服务

提问 路由器使用 DNS 服务器来解析主机名

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip domain-lookup**

Router1(config)#**ip domain-name *oreilly.com***

Router1(config)#**ip name-server *172.25.1.1***

Router1(config)#**ip name-server *10.1.20.5***

Router1(config)#**end**

Router1#

注释 从 IOS 12.2 开始，思科使用了 *ip domain lookup*.来代替 *ip domain-lookup* 类似的 *ip domain-name* 被 *ip domain name* 代替

2.12. 禁用域名解析

提问 禁用域名解析，防止路由器自动对打错的命令的进行 DNS 查询

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**no ip domain-lookup**

Router1(config)#**end**

Router1#

如果需要启用 DNS 查询主机名，但是又为了避免打错命令查询的情况可以使用如下的变通方法

Router1#configure terminal

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#line vty 0 4

Router1(config-line)#transport preferred none

Router1(config-line)#end

Router1#

注释 对后一个命令的稍微解释一下，正常情况下都知道可以直接使用主机名回车路由器会认为是 telnet 到此设备，可以省略掉 telnet 的命令，原因是因为 transport preferred 缺省是 telnet，如果配置为 none 就必须使用 telnet 命令来进行设备登录，命令打错也不会出现地址解析的问题了。

2.13. 配置路由器特定时间重启

提问 需要路由器在特定时间自动重启

回答

Router1#**reload in *20***

Reload scheduled for 11:33:53 EST Sat Feb 1 2003 (in 20 minutes)

Proceed with reload? [confirm] **<enter>**

Router1#

Router1#**reload at *14:00 Feb 2***

Reload scheduled for 14:00:00 EST Sun Feb 2 2003 (in 26 hours and 44 minutes)

Proceed with reload? [confirm] **<enter>**

Router1#

注释 很有用的命令，当你在对路由器配置进行修改前可以先行输入此命令，然后进行修改但是不保存配置，这样可以防止把自己锁在路由器之外。可以使用 **reload cancel** 命令来取消定时重启

2.14. 定时执行配置命令

提问 周期性的定时执行某个命令

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**kron policy-list** *NEOSHI*

Router(config-kron-policy)#**cli** *write memory*

Router(config-kron-policy)#**exit**

Router(config)#**kron occurrence** *DAILYat5* **at** *17:00* **recurring**

Router(config-kron-occurrence)#**policy-list** *NEOSHI*

Router(config-kron-occurrence)#**end**

Router#

注释 从 IOS12.3(1)开始引入了这个类似 Unix Cron 的特性，不过也有一些缺点，只能运行 EXEC 模式下的命令，不能运行配置模式下的命令，同时输入的命令不能是交互性的，比如不能输入 copy running-config startup-config 来保存配置，因为是需要确认的，必须使用 write memory 来代替

2.15. 显示路由器 CPU 利用率的历史数据

提问 显示历史的路由器 CPU 利用率

回答

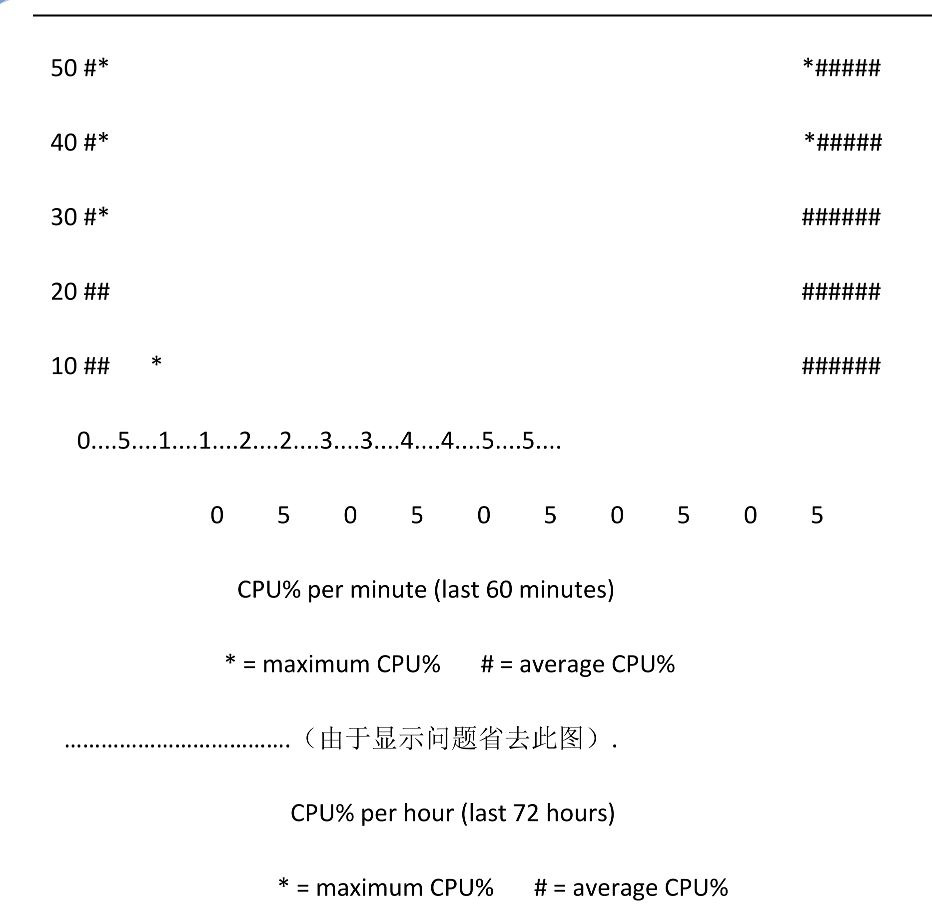
Router# **show processes cpu history**

Router 03:48:18 PM Monday Apr 17 2006 EDT

5555599999999999999999

```
5                                             44444999999999999999
100                                               *****************
90                                                *****************
80                                                *****************
70                                                *****************
60                                                *****************
50                                           *********************
40                                           *********************
30                                           *********************
20                                           *********************
10 *                                        *********************
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
             CPU% per second (last 60 seconds)

    99    1                                                9999
    99    1                                4               9999
100 **                                                     ***#*#
90 **                                                      **##*#
80 #*                                                      *###*#
70 #*                                                      *###*#
60 #*                                                      *###*#
```



```
50 #*                                                    *#####
40 #*                                                    *#####
30 #*                                                    ######
20 ##                                                    ######
10 ##     *                                              ######
   0....5....1....1....2....2....3....3....4....4....5....5....
             0    5    0    5    0    5    0    5    0    5
               CPU% per minute (last 60 minutes)
             * = maximum CPU%    # = average CPU%
 ..................................（由于显示问题省去此图）.
                   CPU% per hour (last 72 hours)
                  * = maximum CPU%    # = average CPU%
```

注释 从 IOS12.2(2)T 以后思科为 show process cpu 命令增加了 history 的选项，这样可以看到最长 3 天的 CPU 利用率，而以前最多可以看到 5 分钟的。输出图很不容易看懂，简单的说最左边是最新的数据，然后历史数据会向右移，在每分钟和每小时的会有峰值和平均值，峰值为现在每列的上端，不过是竖着排列的。

2.16. 生成意外导出文件（EXCEPTION DUMP FILES）

提问 在路由器发生意外当机的情况下生成导出文件发给 TAC 进行处理

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip ftp source-interface *Loopback0***

Router1(config)#**ip ftp username *ijbrown***

Router1(config)#**ip ftp password *ijpassword***

Router1(config)#**exception protocol ftp**

Router1(config)#**exception region-size *65536***

Router1(config)#**exception dump *172.25.1.3***

Router1(config)#**end**

Router1#

注释 缺省情况下路由器会使用 tftp 命令进行传送，不过 TFTP 有 16M 的限制所以建议换为 FTP 协议。另外为了防止当机导致文件不能生成，所以使用了 **exception region-size *65536*** 来提前保留部分内存给该命令使用。可以先使用 **write core** 命令来提前实验下生成此文件

2.17. 生成接口信息报告

2.18. 生成路由表报告

2.19. 生成 ARP 表报告

2.20. 生成主机表报告

以上都是使用 perl 脚本来进行命令输出的汇总操作，脚本略去

第三章 用户访问和权限管理

3.1. 设置用户名和密码

提问 为每个单独的人员设置不同的用户名和密码

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**username *neoshi* password *ioscookbook*** （**username *weak* nopassword**）

Router1(config)#**aaa new-model**

Router1(config)#**aaa authentication login *local_auth*** local

Router1(config)#**line vty 0 4**

Router1(config-line)#**login authentication *local_auth***

Router1(config-line)#**exit**

Router1(config)#**end**

Router1#

注释 设置单独的用户名和密码的好处就不用多说了，这里只提一个就是在日志中会显示谁做了修改，比如%SYS-5-RELOAD: Reload requested **by kdooley** on vty0 (172.25.1.1).另外在 username 这个命令里面还有一个autocommand的选项，实现登录以后自动执行某个特定的命令的作用，下面的例子就是一个用户名为 run 无密码，登录以后显示完端口状态就自动退出的例子，很好用吧

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**aaa new-model**

Router1(config)#**aaa authentication login default local**

Router1(config)#**aaa authorization exec default local**

Router1(config)#**username *run* nopassword noescape**

Router1(config)#**username *run* autocommand *show ip interface brief***

Router1(config)#**end**

Router1#

3.2. 加密密码

提问 加密密码从而在配置文件中不明文显示

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**enable password *oreilly***

Router1(config)#**line vty 0 *4***

Router1(config-line)#**password *cookbook***

Router1(config-line)#**line con 0**

Router1(config-line)#**password *cookbook***

Router1(config-line)#**line aux 0**

Router1(config-line)#**password *cookbook***

Router1(config-line)#**exit**

Router1(config)#**service password-encryption**

Router1(config)#**end**

Router1#

注释 这种加密方式很弱，很容易被破解

3.3. 使用更高强度加密技术

提问 使用强度高的加密方式而不是思科缺省的加密技术

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**enable secret *ORAbooks***

Router1(config)#**end**

Router1#

在 IOS 12.2(8)T 后也可以对 username 的密码做高强度的加密

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**username *ijbrown* secret *oreilly***

Router(config)#**end**

Router#

注释 由于这种加密方式使用的是 MD5 所以破解难度相对增大了。对于 enable secret 的密码有个小技巧就是密码设定正常没有？，不过可以通过^V+？的方式来输入。

3.4. 移去配置文件中的密码信息

提问 不想在配置文件中显示密码

回答 使用脚本略去

注释 简单的用 show tech 命令也可以

3.5. 解密思科的弱密码

提问 破解思科缺省的密码算法

回答 使用脚本略去

注释 可以使用 BOSON 网站上的免费工具

3.6. 显示当前登录用户

提问 显示当前登录设备的用户

回答

Router1#**show users （who）**

注释 无

3.7. 发信息给其它用户

提问 试图发送信息给登录在同一设备的其它用户

回答

Router1#**send ***

Router1#**send console 0**

Router1#**send vty *2***

Router1#**send *66***

注释 很好用的特性，比如当你重启的时候需要告诉别人，文本信息^+Z 结束

3.8. 修改可用 VTY 数目

提问 增加或者减少可登录用户的数目

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**line vty *0 9***

Router1(config-line)#**exit**

Router1(config)#**end**

Router1#

注释 缺省可登录 vty 数目为 5，不能删除，对于增加的可以使用 no line vty x 删除，不能不能删除单独的 vty，是删除所有大于 x 的 vty

3.9. 修改 VTY 的超时时长

提问 修改超时时长避免用户登录超时被系统断开

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**line vty *0 4***

Router1(config-line)#**exec-timeout 0 0** （**exec-timeout *240 0***）

Router1(config-line)#**exit**

Router1(config)#**end**

Router1#

注释 缺省用户 10 分钟空闲就会被踢掉系统，0 0 可以用不超时，第一个 0 是分钟，第二个 0 是秒。同时为了防止有些用户掉死但是还占用 vty 端口的情况，建议使用下面命令来防止：

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**service tcp-keepalives-in**

Router1(config)#**end**

Router1#

3.10. 限制用户登录可以使用的协议

提问 只允许用户用特定的协议来进行系统登录

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**line vty *0 4***

Router1(config-line)#**transport input telnet**

Router1(config-line)#**exit**

Router1(config)#**end**

Router1#

注释 缺省情况下除了可以 telnet 登录，还支持以下协议登录 **lat pad v120 lapb-ta rlogin ssh**

3.11. 配置用户登录可用总时长

提问 对用户登录总时长进行限制，不论是否在空闲还是活动

回答 Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**line vty *0 4***

Router1(config-line)#**absolute-timeout *5***

Router1(config-line)#**logout-warning *30***

Router1(config-line)#**exit**

Router1(config)#**end**

Router1#

注释 无

3.12. 部署 BANNERS

提问 设置登录时显示的警示性信息

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**banner exec** ***# This is an exec banner #***

Router1(config)#**banner login** ***# This is a login banner #***

Router1(config)#**banner motd** ***$ This is a motd banner $***

Router1(config)#**end**

Router1#

注释 不用使用 welcome 之类的字样，下面是一个 FBI 的路由器登录 banner 做参考

Router1(config)#**banner login #**

Enter TEXT message. End with the character '#'.

+---+

| WARNING |

| ------- |

| This system is solely for the use of authorized users for official |

| purposes. You have no expectation of privacy in its use and to |

| ensure that the system is functioning properly, individuals using |

| this computer system are subject to having all of their activities |

| monitored and recorded by system personnel. Use of this system |

| evidences an express consent to such monitoring and agreement that |

| if such monitoring reveals evidence of possible abuse or criminal |

| activity, system personnel may provide the results of such |

| monitoring to appropriate officials. |

+---+

#

Router1(config)#**end**

Router1#

3.13. 在特定端口禁用 BANNERS 显示

提问 aux 口用于 modem 连接，为了避免出现问题希望关闭 banner 显示

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**line aux 0**

Router1(config-line)#**no motd-banner**

Router1(config-line)#**no exec-banner**

Router1(config-line)#**exit**

Router1(config)#**end**

Router1#

注释 无

3.14. 禁用 LINE 登录

提问 禁止在 AUX 或者 Line 端口进行设备登录

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**line aux 0**

Router1(config-line)#**transport input none**

Router1(config-line)#**no exec**

Router1(config-line)#**exec-timeout *0 1***

Router1(config-line)#**no password**

Router1(config-line)#**exit**

Router1(config)#**end**

Router1#

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**access-list *98* deny any log**

Router1(config)#**line vty *0 4***

Router1(config-line)#**transport input none**

Router1(config-line)#**exec-timeout *0 1***

Router1(config-line)#**no exec**

Router1(config-line)#**access-class *98* in**

Router1(config-line)#**exit**

Router1(config)#**end**

Router1#

注释 无

3.15. 为管理员保留特定的登录端口

提问 防止所有的登录端口都被占用，为管理员留一个后门

回答

```
Router1#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router1(config)#access-list 9 permit 172.25.1.1
Router1(config)#line vty 4
Router1(config-line)#access-class 9 in
Router1(config-line)#exit
Router1(config)#end
Router1#
```

或者

```
Router1#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router1(config)#access-list 9 permit 172.25.1.1
Router1(config)#line vty 5 7
Router1(config-line)#rotary 25
Router1(config-line)#access-class 9 in
Router1(config-line)#exit
Router1(config)#end
Router1#
```

注释 在使用第二种 rotary 命令时就相应的改变登录时的端口号码，不是缺省的 23，而是 3000＋rotary 的号码 25＝3025

3.16. 限制特定地址的 TELNET 登录

提问 只允许特定的机器进行 Telnet 登录

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**access-list *99* permit *172.25.1.0 0.0.0.255***

Router1(config)#**access-list *99* deny any log**

Router1(config)#**line vty *0 4***

Router1(config-line)#**access-class *99* in**

Router1(config-line)#**exit**

Router1(config)#**end**

Router1#

注释 无

3.17. 对 TELNET 访问进行日志记录

提问 记录每次 telnet 的日志

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**access-list *90* permit any log**

Router1(config)#**line vty *0 4***

Router1(config-line)#**access-class *90* in**

Router1(config-line)#**exit**

Router1(config)#**end**

Router1#

注释 需要注意的是不管登录成功还是失败，在日志中都是显示的 permitted：

%SEC-6-IPACCESSLOGS: list 90 permitted 172.25.1.1 1 packet

3.18. 设置发起 TELNET 的源地址

提问 有时对端设备有安全设置只允许特定的地址发起 telnet 请求

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip telnet source-interface** ***loopback0***

Router1(config)#***end***

Router1#

或者

Router1#**telnet** ***172.25.1.5*** **/source-interface** ***loopback0***

注释 缺省情况路由器会使用到目的地所使用的端口来做 Telnet 的源地址

3.19. 自动登录

注释 使用脚本略去，其实用 SecueCRT 很容易设定

3.20. 使用 SSH 登录

提问 启用 SSH 这种加密的登录方式

回答

Router1#**configure terminal**

Enter configuration commands, one per line.　End with CNTL/Z.

Router1(config)#**hostname *Router1***

Router1(config)#**ip domain-name *neoshi.net***

Router1(config)#**crypto key generate rsa**

The name for the keys will be: Router1.oreilly.com

Choose the size of the key modulus in the range of 360 to 2048 for your

General Purpose Keys. Choosing a key modulus greater than 512 may take

a few minutes.

How many bits in the modulus [512]: ***1024***

Generating RSA keys ...

[OK]

Router1(config)#

Jun 27 15:04:15: %SSH-5-ENABLED: SSH 1.5 has been enabled

Router1(config)#**ip ssh time-out *120***

Router1(config)#**ip ssh authentication-retries *4***

Router1(config)#**end**

Router1#

注释 从 IOS 12.3(4)T 开始支持 SSH v2，之前只支持 v1，首先要确认你的 IOS 版本，然后确认支持安全特性 3DES，才能开启 SSH 的特性

3.21. 改变 IOS 命令的特权等级

提问 修改特定 IOS 命令的特权等级

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**privilege exec level *1 show startup-config***

Router1(config)#**end**

Router1#

注释 缺省情况路由器支持 16 种特权等级，命令一般归属于 0,1 和 15 三种特权等级，在特权等级 0 下面只支持 disable, enable, exit, help, 和 logout 命令，1 下面不能对配置进行修改，15 就是 enable 的特权等级

3.22. 基于用户的特权等级

提问 给不同的用户赋予不同的特权等级

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**aaa new-model**

Router1(config)#**aaa authentication login default local**

Router1(config)#**aaa authorization exec default local**

Router1(config)#**username *neoshi* privilege *10 password ioscookbook***

Router1(config)#**privilege exec level *10 show ip route***

Router1(config)#**privilege exec level *1 show ip***

Router1(config)#**privilege exec level *1 show***

Router1(config)#**end**

Router1#

注释 通常的 0，1 和 15 三种等级弹性不足，可以定义更多的等级给不同的用户

3.23. 基于端口的特权等级

提问 根据登录的不同端口自动赋予特定的特权等级

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**line *aux 0***

Router1(config-line)#**privilege level *5***

Router1(config-line)#**exit**

Router1(config)#**privilege exec level *5 show ip route***

Router1(config)#**privilege exec level *1 show ip***

Router1(config)#**privilege exec level *1 show***

Router1(config)#**end**

Router1#

注释 无

第四章 TACAS+

4.1. 用户登录集中鉴权

提问 使用集中的鉴权方式对用户登录设备进行控制

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**aaa new-model**

Router1(config)#**aaa authentication login default group tacacs+**

Router1(config)#**aaa authentication enable default group tacacs+**

Router1(config)#**tacacs-server host *172.25.1.1***

Router1(config)#**tacacs-server key *COOKBOOK***

Router1(config)#**end**

Router1#

注释 部署集中化鉴权就不需要在每台设备上配置用户名密码了，改密码也变的简单了

4.2. 限制特定命令的执行权限

提问 对设备可执行命令权限进行基于用户的授权

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**aaa new-model**

Router1(config)#**aaa authorization exec default group tacacs+**

Router1(config)#**aaa authorization commands *15* default group tacacs+**

Router1(config)#**tacacs-server host *172.25.1.1***

Router1(config)#**tacacs-server key *neoshi***

Router1(config)#**end**

Router1#

注释 无

4.3. TACACS+服务器无法访问

提问 防止出现 TACACS+服务器故障导致所有用户都不能登录

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**aaa new-model**

Router1(config)#**aaa authentication login default group tacacs+ enable**

Router1(config)#**aaa authentication enable default group tacacs+ enable**

Router1(config)#**aaa authorization commands *15* default group tacacs+ if-authenticated**

Router1(config)#**tacacs-server host *172.25.1.1***

Router1(config)#**tacacs-server key *COOKBOOK***

Router1(config)#**end**

Router1#

注释 在认证服务器出现故障的情况下使用 enable 密码作为备份，同时建议使用 **if-authenticated** 参数在你配置授权的时候

4.4. 在特定端口禁用 TACACS+鉴权

提问 为了方便禁止在控制口使用 TACACS+鉴权

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**aaa new-model**

Router1(config)#**aaa authentication login default group tacacs+ local**

Router1(config)#**aaa authentication login *NEOSHI* line**

Router1(config)#**line con 0**

Router1(config-line)#**login authentication *NEOSHI***

Router1(config-line)#**end**

Router1#

注释 无

4.5. 记录用户行为

提问 记录用户输入的配置命令和时间

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**aaa new-model**

Router1(config)#**aaa accounting commands *1* default stop-only group tacacs+**

Router1(config)#**aaa accounting commands *15* default stop-only group tacacs+**

Router1(config)#**end**

Router1#

注释 下面是一条日志记录，很详尽吧

Fri Jan 3 11:08:47 2006 toronto ijbrown tty66 172.25.1.1 stop task_id=512 start_time=1041610127 timezone=EST service=shell priv-lvl=15 cmd=configure terminal <cr>

4.6. 记录系统事件

提问 记录系统事件

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**aaa new-model**

Router1(config)#**aaa accounting exec default start-stop group tacacs+**

Router1(config)#**aaa accounting connection default start-stop group tacacs+**

Router1(config)#**aaa accounting system default stop-only group tacacs+**

Router1(config)#**end**

Router1#

注释 除了可以记录用户输入命令以外还提供了 exec（用户开始和中止 exec 会话的时间记录），connection（用户发起外部连接的时间，地址，数据包多少等信息记录比如 telnet ssh 等）和 system（系统重启，禁用 AAA 等系统信息）等三种系统事件的记录

4.7. 设置 TACACS+消息的源地址

提问 发送 TACACS+消息时只使用特定的源地址

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip tacacs source-interface *Loopback0***

Router1(config)#**end**

Router1#

注释 所有本设备的记录都来自于同一地址方便对日志进行汇总和统计

4.8. TACACS+服务器配置文件样本

注释 可以使用思科免费的 TACACS+服务器也可以使用商业的服务器，配置方式略

第五章 IP 路由

5.1. 查找路由条目

提问 在路由表中查找特定的路由条目

回答

Router>**show ip route *172.25.100.15***

```
Routing entry for 172.25.100.0/24
  Known via "ospf 55", distance 110, metric 11, type inter area
  Redistributing via ospf 55
  Last update from 172.25.1.1 on Ethernet0, 2d12h ago
  Routing Descriptor Blocks:
  * 172.25.1.1, from 172.25.1.1, 2d12h ago, via Ethernet0
      Route metric is 11, traffic share count is 1
```

注释 路由器在路由表中查找路由条目的原则是最长匹配，所以例子中虽然查找的是 172.25.200.15 但是由于没有这条特定的路由，显示的结果是最长匹配的 172.15.100.0/24。如果没有任何一条匹配只能使用缺省路由，会出现下面信息

Router> **show ip route *172.15.101.5***

% Network not in table

注意的是这里都是无类路由，如果有类的就不一样了

5.2. 查找特定类型的路由条目

提问 在路由表中查找相同类型的路由条目

回答

Router>**show ip route static**

192.168.1.0/32 is subnetted, 1 subnets

S 192.168.1.1 [1/0] via 172.25.1.4

还有一个更有用的命令

Router>**show ip route summary**

IP routing table name is Default-IP-Routing-Table(0)

Route Source	Networks	Subnets	Overhead	Memory (bytes)
connected	0	3	328	432
static	1	0	64	144
ospf 55	1	3	256	576
Intra-area: 1 Inter-area: 2 External-1: 1 External-2: 0				
NSSA External-1: 0 NSSA External-2: 0				
internal	2			2328
Total	4	6	648	3480

注释 通过显示路由表的统计情况来了解当前路由器的路由条目，也可以用来以后的比对

5.3. 各种掩码的转换

注释 脚本略去，建议使用 Boson 提供的免费转换工具

5.4. 使用静态路由

提问 配置静态路由

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**ip route *10.35.15.5 255.255.255.255* Ethernet0 （permanent 选项可以使此条目一直存在于路由表中，而不管下一跳的可达性）**

Router(config)#**ip route *172.16.0.0 255.255.0.0 10.35.6.1 2*** **（permanent）**

Router(config)#**end**

Router#

也可以给路由条目打上标签

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**ip route *172.16.0.0 255.255.0.0 10.35.6.1 2* tag *36291***

Router(config)#**end**

Router#

注释 在类似以太网这种多路访问的网络中建议使用下一跳为地址而不是接口。正常情况下路由器对静态路由的下一跳有效性的检查是一分钟，在 12.3(10)以后增加了下面的命令可以对此时间进行调整 Router(config)#**ip route static adjust-time *30***。对静态路由打 tag 用于路由再发布时的区分

5.5. 浮动静态路由

提问 当动态路由出问题的时候使用静态路由作为备份

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**ip route** ***10.0.0.0 255.0.0.0 172.16.1.1*** **190** （下一跳也可以触发一个拨号接口）

Router(config)#**end**

Router#

注释 通过调整管理距离的方式来进行路由备份，不过要注意的是管理距离只适合在相同路由的情况下，路由条目的最长匹配是第一位的。另外在不同厂商设备互联的时候，调整管理距离一定要设置合理。

5.6. 基于源地址的策略路由

提问 根据源地址的不同选择不同的路径

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**access-list** ***1*** **permit** ***10.15.35.0 0.0.0.255***

Router(config)#**access-list** ***2*** **permit** ***10.15.36.0 0.0.0.255***

Router(config)#**interface** ***Ethernet0***

Router(config-if)#**ip address** ***10.15.22.7 255.255.255.0***

Router(config-if)#**ip policy route-map** ***Engineers***

Router(config-if)#**ip route-cache policy**

Router(config-if)#**exit**

Router(config)#**route-map** ***Engineers*** **permit** ***10***

Router(config-route-map)#**match ip address** ***1***

Router(config-route-map)#**set ip next-hop** ***10.15.27.1***

Router(config-route-map)#**exit**

Router(config)#**route-map *Engineers* permit *20***

Router(config-route-map)#**match ip address *2***

Router(config-route-map)#**set interface *Ethernet1***

Router(config-route-map)#**end**

Router#

注释 缺省情况下 route map 的最后一句都是 deny all，这样不符合 route map 规则的数据包都会按照正常的路由表进行转发。**set ip next-hop verify-availability** 命令提供了对下一跳的验证，不过是基于 CDP 的，所以如果使用此命令需要打开 CDP，最好同时调整时长，毕竟缺省是 180 秒。在使用策略路由时会在排错时增加难度，因为缺省对于本路由器发出的数据包可以绕过 route map 这样会造成错觉。

5.7. 基于应用的策略路由

提问 根据不同的应用来选择不同的路径

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**access-list *101* deny tcp *10.15.25.0 0.0.0.255* any eq *www***

Router(config)#**access-list *101* permit tcp any any eq *www***

Router(config)#**interface *Ethernet0***

Router(config-if)#**ip address *10.15.22.7 255.255.255.0***

Router(config-if)#**ip policy route-map *Websurfers***

Router(config-if)#**ip route-cache policy**

Router(config-if)#**exit**

Router(config)#**route-map *Websurfers* permit *10***

Router(config-route-map)#**match ip address *101***

Router(config-route-map)#**set ip next-hop *10.15.27.1***

Router(config-route-map)#**exit**

Router(config)#**route-map *Websurfers* permit *20***

Router(config-route-map)#**set ip default next-hop *10.15.26.1***

Router(config-route-map)#**end**

Router#

对于本设备的发出的数据包也使用策略路由

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**ip local policy route-map *dlswtraffic***

Router(config)#**access-list *103* permit tcp any any eq *2065***

Router(config)#**access-list *103* permit tcp any eq *2065* any**

Router(config)#**route-map *dlswtraffic* permit *10***

Router(config-route-map)#**match ip address *103***

Router(config-route-map)#**set ip next-hop *10.15.27.3***

Router(config-route-map)#**end**

Router#

注释 正常情况下如果所有定义的下一跳都不存在的情况下会使用路由表来查询，如果路由表没有此定义会使用缺省路由，这时候你可以使用 **set ip default next-hop** 来定义一个不同的缺省路由

5.8. 策略路由检查

提问 检查所应用的策略路由

回答

```
Router>show ip policy
Interface        Route map
local            dlswtraffic
Ethernet0        Websurfers
Serial0          High-priority
Router>show route-map
route-map High-priority, permit, sequence 10
  Match clauses:
    ip address (access-lists): 101
  Set clauses:
    ip next-hop 10.15.27.1
  Policy routing matches: 0 packets, 0 bytes
route-map Websurfers, permit, sequence 10
  Match clauses:
    ip address (access-lists): 102
  Set clauses:
    ip next-hop 10.15.27.1
  Policy routing matches: 0 packets, 0 bytes
route-map Websurfers, permit, sequence 20
  Match clauses:
  Set clauses:
```

```
        ip default next-hop 10.15.26.1
    Policy routing matches: 4 packets, 531 bytes
route-map dlswtraffic, permit, sequence 10
    Match clauses:
        ip address (access-lists): 103
    Set clauses:
        ip next-hop 10.15.27.3
    Policy routing matches: 5 packets, 500 bytes
```

注释 也可以通过 **show access-list 103** 命令看到更多的匹配信息

5.9. 改变管理距离

提问 调整学到的外部网络的缺省管理距离

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**router rip**

Router(config-route)#**network *192.168.15.0***

Router(config-route)#**distance *15 192.168.15.1 0.0.0.0***

Router(config-route)#**distance *200 192.168.15.0 0.0.0.255***

Router(config-route)#**distance *255***

Router(config-route)#**end**

Router#

```
Router#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router(config)#router eigrp 111
Router(config-route)#network 192.168.16.0
Router(config-route)#distance eigrp 55 200
Router(config-route)#end
Router#
Router#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router(config)#router ospf 66
Router(config-route)#distance ospf inter-area 115
Router(config-route)#distance ospf intra-area 105
Router(config-route)#distance ospf external 125
Router(config-route)#end
Router#
Router#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router(config)#router bgp 65520
Router(config-route)#distance bgp 115 220 50
Router(config-route)#end
Router#
```

注释 管理距离只是针对自己的，通过调整这些外部路由的管理距离来调整自己路由表的结构

5.10. 相同代价值的多路径路由

提问 限制路由器到达同一目的地的路径数目

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**router ospf *65510***

Router(config-router)#**maximum-paths *2***

Router(config-router)#**end**

Router#

IOS 12.2T 以后对 BGP 增加了下面的命令

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**router bgp *65511***

Router(config-router)#**maximum-paths *2***

Router(config-router)#**maximum-paths ibgp *3***

Router(config-router)#**end**

Router#

注释 缺省情况下静态路由可以有 6 条冗余，BGP 只有一条最佳路径，其他路由协议为 4 条。使用上述命令在 12.3(2)T 之前可以调整最大为 6 条，12.3(2)T 之后可以最大为 16 条

5.11. 配置静态路由的追踪

提问 在某个端口当掉等情况下才启用特定的静态路由

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**track *10* interface *Serial0/0* line-protocol**

Router(config-track)#**delay down *5* up *30***

Router(config-track)#**exit**

Router(config)#**ip route *192.168.10.0 255.255.255.0 10.3.12.26* track *10***

Router(config)#**end**

Router#

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**track *11* ip route *10.2.95.0 255.255.255.0* reachability**

Router(config-track)#**delay down *5* up *5***

Router(config-track)#**exit**

Router(config)#**ip route *0.0.0.0 0.0.0.0 10.3.12.26* track *11***

Router(config)#**end**

Router#

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**track *12* list boolean and**

Router(config-track)#**object *10* not**

Router(config-track)#**object *11***

Router(config-track)#**exit**

Router(config)#**ip route *192.168.13.0 255.255.255.0 10.3.12.26* track *12***

Router(config)#**end**

Router#

注释 从 12.3T 和 12.4 以后开始 IOS 提供了一种 track 的特性，可以定义跟踪不同的状态。可以使用 show track 命令来查看跟踪的状态。跟踪状态也可以进行组合，使用 and or 逻辑运算或者百分比，权重等增加灵活度，很好玩，不过别把自己绕进去了

5.12. 路由表变动统计

提问 通过路由表变动的统计来衡量路由表的稳定性

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**ip route profile**

Router(config)#**end**

Router#

Router#**show ip route profile**

IP routing table change statistics:

Frequency of changes in a 5 second sampling interval

Change/ Fwd-path Prefix Nexthop Pathcount Prefix

interval change add change change refresh

----

0 327 327 335 335 331

1	4	4	0	0	1
2	2	2	0	0	1
3	0	0	0	0	0
4	1	1	0	0	1

....

Router#

注释 12.0 就有的一个老命令，但估计很少有人使用，这个统计也是够难懂的，简单的说最理想的情况就是第一行数目很大，其他行都是 0。统计方法是每 3 秒一个间隔，在这个间隔内如果有 1 次路由表变化就累计一次，多次变化就累计多次。但这个命令还是有一些缺点，一就是不能清掉老的数据，必须通过 **no ip route profile**，然后 **ip route profile** 来清除，还有就是这里只是统计结果，没有办法确定是哪条路由出的问题

第六章 RIP

6.1. 配置 RIP（V1）

提问 在简单的网络中启用 RIP 路由协议

回答

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**interface *Ethernet0***

Router2(config-if)#**ip address *192.168.30.1 255.255.255.0***

Router2(config-if)#**interface *Serial0.1***

Router2(config-subif)#**ip address *172.25.2.2 255.255.255.0***

Router2(config-subif)#**exit**

Router2(config)#**router rip**

Router2(config-router)#**network *172.25.0.0***

Router2(config-router)#**network *192.168.30.0***

Router2(config-router)#**exit**

Router2(config)#**end**

Router2#

注释 要特别注意的是版本 1 的 RIP 中的 network 命令是无类的，就算你配置命令是有类的网络，路由器内部还是会转化为无类的。**show ip rip database** 是一个很好的验证命令

6.2. RIP 中的路由过滤

提问 限制 RIP 中某些特定路由条目的交换

回答

入方向

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**access-list *10* deny *192.168.20.0***

Router2(config)#**access-list *10* permit any**

Router2(config)#**router rip**

Router2(config-router)#**distribute-list *10* in *Serial 0.1*** *（该命令除了可以用于特定接口也可以用于所有接口）*

Router2(config-router)#**network *172.25.0.0***

Router2(config-router)#**network *192.168.30.0***

Router2(config-router)#**exit**

Router2(config)#**end**

Router2#

出方向

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**access-list *20* permit *0.0.0.0***

Router1(config)#**access-list *20* deny any**

Router1(config)#**router rip**

Router1(config-router)#**distribute-list *20* out *Serial0/0.2***

Router1(config-router)#**network *172.25.0.0***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 使用 **show ip protocol** 命令可以用来验证所配置的 distribute-list

6.3. 再发布静态路由至 RIP

提问 再发布你所配置的静态路由到 RIP 路由协议中

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip route *192.168.10.0 255.255.255.0 172.22.1.4***

Router1(config)#**router rip**

Router1(config-router)#**redistribute static metric *5***

Router1(config-router)#**distribute-list *7* out static**

Router1(config-router)#**exit**

Router1(config)#**access-list *7* permit *192.168.10.0***

Router1(config)#**end**

Router1#

注释 这里再发布还是要注意无类路由的问题，所以还是建议用 V2。例子是再发布静态路由，也可以再发布其他动态路由协议，比如 OSPF，BGP，EIGRP 等，命令类似 **redistribute eigrp *65530***

有一个好玩的情况是虽然此命令也可以支持 RIP 自己的再发布，但是配置时候是不允许的，因为 RIP 没有其他动态路由协议中的进程号的概念，无法区别不同的进程

6.4. 使用 ROUTE MAPS 进行路由再发布

提问 使用 Route Maps 这种更好控制粒度的方式来进行路由再发布的配置

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip route *192.168.10.0 255.255.255.0 172.22.1.4***

Router1(config)#**ip route *192.168.11.0 255.255.255.0 172.22.1.4***

Router1(config)#**ip route *192.168.12.0 255.255.255.0 172.22.1.4***

Router1(config)#**access-list *20* permit *192.168.10.0***

Router1(config)#**access-list *21* permit *192.168.11.0***

Router1(config)#**route-map *STATIC* permit *10***

Router1(config-route-map)#**match ip address *20***

Router1(config-route-map)#**set metric *2***

Router1(config-route-map)#**set tag *2***

Router1(config-route-map)#**exit**

Router1(config)#**route-map *STATIC* permit *20***

Router1(config-route-map)#**match ip address *21***

Router1(config-route-map)#**set metric *8***

Router1(config-route-map)#**route-map *STATIC* deny *30***

Router1(config-route-map)#**exit**

Router1(config)#**router rip**

Router1(config-router)#**redistribute static route-map *STATIC***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 使用 route map 可以对路由再发布进行更好粒度的控制，如果觉的配置命令难懂的话，使用验证命令 **show route-map** 可能更好理解一些

6.5. 在 RIP 中宣告缺省路由

提问 使用 RIP 来宣告一条缺省路由

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip route 0.0.0.0 0.0.0.0 *172.25.1.1***

Router1(config)#**router rip**

Router1(config-router)#**default-information originate**

Router1(config-router)#**end**

Router1#

或者使用再发布命令

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip route 0.0.0.0 0.0.0.0 *172.25.1.1***

Router1(config)#**access-list *7* permit *0.0.0.0***

Router1(config)#**router rip**

Router1(config-router)#**redistribute static**

Router1(config-router)#**distribute-list *7* out static**

Router1(config-router)#**end**

Router1#

注释 推荐使用第一种方式，除了可以免除使用过滤列表以外还可以和 route map 来组合使用

6.6. 在特定接口禁用 RIP

提问 阻止某个接口参与 RIP

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**access-list *12* deny any**

Router1(config)#**router rip**

Router1(config-router)#**passive-interface *FastEthernet0/1***

Router1(config-router)#**distribute-list** ***12*** **in** ***FastEthernet0/1***

Router1(config-router)#**end**

Router1#

注释 ***passive-interface*** 用于防止端口发送路由信息，但是并不能控制此接口不接收路由信息，所以要再使用 ***distribute-list*** 命令来防止此接口接收路由信息

6.7. 缺省被动接口

提问 缺省在所有端口禁用 RIP，除非特别指定

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**router rip**

Router1(config-router)#**passive-interface default**

Router1(config-router)#**no passive-interface** ***FastEthernet0/0.1***

Router1(config-router)#**network** ***172.22.0.0***

Router1(config-router)#**network** ***172.25.0.0***

Router1(config-router)#**network** ***192.168.1.0***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 无

6.8. RIP 更新使用单播包

提问 不想使用组播或者广播的形式来发布路由更新

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**router rip**

Router1(config-router)#**passive-interface *FastEthernet0/1***

Router1(config-router)#**neighbor *172.22.1.4***

Router1(config-router)#**end**

Router1#

注释 缺省 V1 使用广播包，V2 使用组播包的形式来发布路由更新

6.9. 对路由应用 OFFSETS

提问 修改特定接口学到或者发布路由的度量值

回答

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**access-list *22* permit *192.168.20.0***

Router2(config)#**access-list 33 permit 192.168.30.0**

Router2(config)#**router rip**

Router2(config-router)#**offset-list 33 out *10 Serial0.1***

Router2(config-router)#**offset-list *22* in *5 Serial0.1***

Router2(config-router)#**exit**

Router2(config)#**end**

Router2#

注释 RIP 是根据跳数来进行选路而没有考虑到链路的不同，通过这样的命令可以变相的增加某个接口的度量值，从而在选路时考虑，注意的是 offset 只能增加度量值不能减少

6.10. 定时器调整

提问 对 RIP 的定时器设定进行调整，提高收敛速度

回答

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**router rip**

Router2(config-router)#**timers basic *20 80 80 120***

Router2(config-router)#**exit**

Router2(config)#**end**

Router2#

注释 所有定时器单位都是秒，第一个为更新周期，第二个为无效路由时间，第三个为保持时间，第四个为 flush 时间。需要注意的是要确保启用 RIP 的网络定时器都设置一致

6.11. 增大路由更新数据包发送延迟

提问 避免路由更新数据包发送速度太快导致老设备来不及处理

回答

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**router rip**

Router2(config-router)#**output-delay** 10

Router2(config-router)#**exit**

Router2(config)#**end**

Router2#

注释 正常情况下一个 RIP 更新数据包大小为 512 字节可以包含 25 条路由条目，如果路由表条目大于 25 就会通过多个路由更新包来发送，正常是尽可能快的发，启用本特性可以增加发送的间隔，单位为毫秒

6.12. 启用非周期性更新

提问 避免使用每 30 秒的周期性更新，使用触发更新

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *Serial0/0.2***

Router1(config-subif)#**ip rip triggered**

Router1(config-subif)#**end**

Router1#

注释 一定要在邻居路由器上也启用此特性，只能用于点对点链路

6.13. 增大 RIP 的输入队列

提问 在低端路由器上增加 RIP 的输入队列避免丢失路由信息

回答

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**router rip**

Router2(config-router)#**input-queue *200***

Router2(config-router)#**end**

Router2#

注释 类似 6.11

6.14. 配置 RIP（V2）

提问 启用更灵活的版本 2 RIP

回答

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**router rip**

Router2(config-router)#**version *2***

Router2(config-router)#**network *172.25.0.0***

Router2(config-router)#**network *192.168.30.0***

Router2(config-router)#**end**

Router2#

注释 缺省情况下路由器会监听 v1 和 v2 的 RIP 数据包，但是只会发送 v1 的数据包

6.15. 启用 RIP 认证

提问 对 RIP 的数据包进行认证增加安全性

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**key chain *ORA***

Router1(config-keychain)#**key *1***

Router1(config-keychain-key)#**key-string *neoshi***

Router1(config-keychain-key)#**exit**

Router1(config)#**interface *FastEthernet0/0.1***

Router1(config-subif)#**ip rip authentication key-chain *ORA***

Router1(config-subif)#**ip rip authentication mode text （或者 ip rip authentication mode md5）**

Router1(config-subif)#**exit**

Router1(config)#**end**

Router1#

注释 RIP 认证是 RIPv2 的特性之一，需要注意的是由于启用了认证所以在更新数据包中所包含的路由条目数会减少，文本方式会减少为 24，MD5 会减少为 23

6.16. 配置 RIP 路由汇总

提问 通过使用路由汇总来减少路由表的大小，增加稳定性

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *Serial0/0.2***

Router1(config-subif)#**ip summary-address rip *172.25.0.0 255.255.0.0***

Router1(config-subif)#**exit**

Router1(config)#**end**

Router1#

缺省情况下 RIP 会自动对路由条目汇总为无类网络路由，使用下面方法关闭

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**router rip**

Router1(config-router)#**no auto-summary**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 只要配置的汇总路由中的有一条子网路由是存在的，路由器就会继续宣告此条汇总路由

6.17. 路由标签

提问 对再发布的路由配置标签，从而避免不同路由协议之间路由再发布出现路由回环

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip route *0.0.0.0 0.0.0.0 172.25.1.1***

Router1(config)#**access-list *7* permit *0.0.0.0***

Router1(config)#**route-map *TAGGING* permit *10***

Router1(config-route-map)# **match ip address *7***

Router1(config-route-map)# **set tag *5***

Router1(config-route-map)#**exit**

Router1(config)#**router rip**

Router1(config-router)#**redistribute static route-map *TAGGING***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 标签 TAG 只用于外部的路由，而不是通过 RIP 学到的路由，RIP 自身正常情况下也不直接使用这些标签，只是分发而已，如果这些路由再被分发到其他路由进程就可以用标签来识别从而进行控制

第七章 EIGRP

7.1. 配置 EIGRP

提问 配置网络使用 EIGRP 路由协议

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *Ethernet0***

Router1(config-if)#**ip address *192.168.20.1 255.255.255.0***

Router1(config-if)#**exit**

Router1(config)#**interface *Serial0.1* point-to-point**

Router1(config-subif)#**ip address *172.25.2.2 255.255.255.252***

Router1(config-subif)#**exit**

Router1(config)#**router eigrp *55***

Router1(config-router)#**network *172.25.0.0***

Router1(config-router)#**network *192.168.20.0***

```
Router1(config-router)#exit
Router1(config)#end
Router1#
```

注释 要确保启用此路由协议的所有路由器配置的 EIGRP 后面的进程号相同，可以使用 **show ip eigrp neighbors** 来验证邻居关系。同时支持 **network *192.168.20.0 0.0.0.255*** 来定义发布的网络

7.2. 路由过滤

提问 对 EIGRP 学到或者宣告的路由进行过滤

回答

入方向过滤

```
Router2#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router2(config)#access-list 34 deny 192.168.30.0
Router2(config)#access-list 34 permit any
Router2(config)#router eigrp 55
Router2(config-router)#distribute-list 34 in Serial0.1
Router2(config-router)#exit
Router2(config)#end
Router2#
```

出方向过滤

```
Router1#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router1(config)#access-list 57 permit 172.25.1.0
```

Router1(config)#**access-list *57* deny any**

Router1(config)#**router eigrp *55***

Router1(config-router)#**distribute-list *57* out *Serial0/0.2***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

使用 prefix 方式过滤，并且支持 *gateway* 选项

Router9#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router9(config)#**ip prefix-list *ALLOWED-PREFIXES* permit *10.0.0.0/8* le *32***

Router9(config)#**ip prefix-list *ALLOWED-PREFIXES* deny *0.0.0.0/0* le *32***

Router9(config)#**ip prefix-list *ALLOWED-NEIGHBORS* permit *172.18.19.1/32***

Router9(config)#**ip prefix-list *ALLOWED-NEIGHBORS* permit *172.18.19.4/32***

Router9(config)#**ip prefix-list *ALLOWED-NEIGHBORS* deny *0.0.0.0/0* le *32***

Router9(config)#**router eigrp *55***

Router9(config-router)#**distribute-list prefix *ALLOWED-PREFIXES* gateway *ALLOWED-NEIGHBORS* in**

Router9(config-router)#**exit**

Router9(config)#**end**

Router9#

注释 在路由过滤时推荐使用 prefix 方式而不用 ACL 形式。Gateway 参数只能用于入方向控制，同时建议不用和 interface 混和使用

7.3. 再发布路由到 EIGRP

提问 再发布其他方式学到的路由到 EIGRP 路由进程

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**router eigrp *55***

Router1(config-router)#**redistribute rip**

Router1(config-router)#**default-metric *1000 100 250 100 1500***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 如果再发布的是静态路由可以不用配置 default-metric 命令，对于其他协议都必须配置此命令否则无法成功再发布。再发布之前也可以使用过滤列表进行路由过滤，从而只再发布特定路由

Router1(config)#**router eigrp *55***

Router1(config-router)#**redistribute ospf *99***

Router1(config-router)#**distribute-list *7* out ospf *99***

7.4. 使用 ROUTE MAP 方式来配置再发布

提问 使用控制粒度更好的 Route Map 方式来配置再发布

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip route *192.168.10.0 255.255.255.0 172.22.1.4***

Router1(config)#**ip route *192.168.11.0 255.255.255.0 172.22.1.4***

Router1(config)#**ip route** ***192.168.12.0 255.255.255.0 172.22.1.4***

Router1(config)#**access-list** ***20*** **permit** ***192.168.10.0***

Router1(config)#**access-list** ***21*** **permit** ***192.168.11.0***

Router1(config)#**route-map** ***STATIC*** **permit** ***10***

Router1(config-route-map)#**match ip address** ***20***

Router1(config-route-map)#**set metric** ***56 100 255 1 1500***

Router1(config-route-map)#**set tag** ***2***

Router1(config-route-map)#**exit**

Router1(config)#**route-map** ***STATIC*** **permit** ***20***

Router1(config-route-map)#**match ip address** ***21***

Router1(config-route-map)#**set metric** ***128 200 255 1 1500***

Router1(config-route-map)#**exit**

Router1(config)#**route-map** ***STATIC*** **deny** ***30***

Router1(config-route-map)#**exit**

Router1(config)#**router eigrp** ***55***

Router1(config-router)#**redistribute static route-map** ***STATIC***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 此处配置和前面 6.3 的配置差不多，唯一需要注意的就是前面提到的必须要加上 metric 的设置

7.5. 特定接口禁止 EIGRP

提问 禁止某个端口参与 EIGRP

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**router eigrp *55***

Router1(config-router)#**passive-interface *Serial0/1***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 这里的被动接口和 RIP 不同，由于结果是不能形成邻居在此接口所以使用该命令以后就不能发送也不能接收路由信息

7.6. 调整 EIGRP 度量值

提问 修改学到的 EIGRP 路由器度量值

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**access-list *22* permit *192.168.30.0***

Router1(config)#**access-list *33* permit *192.168.30.0***

Router1(config)#**router eigrp *55***

Router1(config-router)#**offset-list *33* out *10000 Serial0.1***

Router1(config-router)#**offset-list *22* in *10000 Serial0.1***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 无

7.7. 定时器调整

提问 调整定时器优化收敛

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *Serial0.1***

Router1(config-subif)#**ip hello-interval eigrp *55 3***

Router1(config-subif)#**ip hold-time eigrp *55 9***

Router1(config-subif)#**exit**

Router1(config)#**end**

Router1#

注释 EIGRP 的一个特性就是定时器的调整可以基于端口，并且不用保持整个网络中所有设备的定时器设置一致，各个定时器都是独立的

7.8. 启用 EIGRP 认证

提问 增强路由信息安全性

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**key chain *ORA***

Router1(config-keychain)#**key *1***

Router1(config-keychain-key)#**key-string *oreilly***

Router1(config-keychain-key)#**exit**

Router1(config-keychain)#**exit**

Router1(config)#**interface *Serial0/1***

Router1(config-if)#**ip authentication mode eigrp *55* md5**

Router1(config-if)#**ip authentication key-chain eigrp *55 ORA***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 注意这里只是认证不是加密路由信息包。下面提供一种更改 key 方法，帮助网络平稳过渡到新的 key

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**key chain *Mars***

Router1(config-keychain)#**key *1***

Router1(config-keychain-key)#**key-string *rocket***

Router1(config-keychain-key)#**accept-lifetime *00:00:00 Jan 1 1993 00:15:00 Nov 1 2006***

Router1(config-keychain-key)#**send-lifetime *00:00:00 Jan 1 1993 00:00:00 Nov 1 2006***

Router1(config-keychain-key)#**key *2***

Router1(config-keychain-key)#**key-string *martian***

Router1(config-keychain-key)#**accept-lifetime *23:45:00 Oct 31 2006* infinite**

Router1(config-keychain-key)#**send-lifetime** ***00:00:00 Nov 1 2006*** **infinite**

Router1(config-keychain-key)#**end**

Router1#

7.9. 配置 EIGRP 路由汇总

提问 通过路由汇总来减少路由表大小和增强稳定性

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface** ***Serial0/0.2***

Router1(config-subif)#**ip summary-address eigrp** ***55 172.25.0.0 255.255.0.0***

Router1(config-subif)#**exit**

Router1(config)#**end**

Router1#

缺省会自动路由汇总，使用 **no auto-summary** 关闭（12.2(8)T 后自动关闭）

同时可以配置汇总路由的同时，宣告部分子网路由

Router9# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router9(config)#**ip prefix-list** ***10.5.5/24*** **permit** ***10.5.5.0/24***

Router9(config)#**route-map** ***LEAK10-5-5*** **permit** ***10***

Router9(config-route-map)#**match ip address prefix-list** ***10.5.5/24***

Router9(config-route-map)#**exit**

Router9(config)#**interface Serial*0/0***

Router9(config-if)#**ip summary-address eigrp 55 10.5.0.0 255.255.0.0 leak-map *LEAK10-5-5***

Router9(config-if)#**exit**

Router9(config)#**end**

Router9#

注释 路由汇总也是 EIGRP 的特性之一，可以配置在任意路由器的接口进行汇总，不象 OSPF 那样只能在 ABR 汇总。汇总路由的度量值和所汇总路由中的最好的子网路由的度量值一致。Leakmap 特性在 12.3(14)T 后引入，可以在汇总路由的同时发布某些更匹配的路由

7.10. 记录邻居状态变化

提问 记录邻居状态变化

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**router eigrp *55***

Router1(config-router)#**eigrp log-neighbor-changes**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 缺省开启

7.11. 限制 EIGRP 路由更新占用带宽

提问 限制 EIGRP 路由更新占用带宽的百分比

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface *Serial0.1***

Router1(config-subif)#**ip bandwidth-percent eigrp *55 40***

Router1(config-subif)#**exit**

Router1(config)#**end**

Router1#

注释 这里的百分比可以大于 100%，当我们人为的设定了某端口带宽用于计算度量值时

7.12. EIGRP STUB 路由

提问 向边缘网络发布较小的路由表

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**router eigrp *55***

Router1(config-router)#**eigrp stub**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 无

7.13. 路由标签

提问 通过对特定路由进行标签，防止再分发时出现路由回环

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip route *0.0.0.0 0.0.0.0 172.25.1.1***

Router1(config)#**access-list *7* permit *0.0.0.0***

Router1(config)#**route-map *TAGGING* permit *10***

Router1(config-route-map)#**match ip address *7***

Router1(config-route-map)#**set tag *5***

Router1(config-route-map)#**exit**

Router1(config)#**router eigrp *55***

Router1(config-router)#**redistribute static route-map *TAGGING***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 无

7.14. 查看 EIGRP 状态

提问 查看状态命令

回答

Router1#**show ip protocols**

Router1#**show ip route eigrp**

Router1#**show ip eigrp neighbors**

Router1#**show ip eigrp interfaces**

Router9#**show ip eigrp accounting**

Router1#**show ip eigrp topology**

注释 12.3(14)T 引入了 *show ip eigrp accounting*

```
Router9#show ip eigrp accounting
IP-EIGRP accounting for AS(55)/ID(172.18.5.9)
Total Prefix Count: 50    States: A-Adjacency, P-Pending, D-Down
State Address/Source      Interface          Prefix     Restart    Restart/
                                                  Count      Count      Reset(s)
 A       172.20.10.1        Se0/0                   1          0          0
 A       172.18.19.1        Fa0/0                  39          0          0
 A       172.18.19.4        Fa0/0                   1          0          0
 A       172.18.19.6        Fa0/0                   6          0          0
Router9#
```

```
Router1#show ip eigrp topology
IP-EIGRP Topology Table for AS(55)/ID(172.25.25.1)


Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status


P 0.0.0.0/0, 1 successors, FD is 28160, tag is 5
         via Rstatic (28160/0)
```

```
        via Summary (28160/0), Null0
P 10.2.2.0/24, 1 successors, FD is 156160
        via 172.22.1.4 (156160/128256), FastEthernet0/1
P 10.1.1.0/30, 1 successors, FD is 3845120
        via Connected, Serial0/1
P 192.168.10.0/24, 1 successors, FD is 28160, tag is 5
        via Rstatic (28160/0)
P 192.168.30.0/24, 1 successors, FD is 156160
        via 172.22.1.4 (156160/128256), FastEthernet0/1
P 192.168.20.0/24, 1 successors, FD is 2195456
        via 172.25.2.2 (2195456/281600), Serial0/0.2
P 172.25.25.6/32, 1 successors, FD is 156160
        via 172.25.1.7 (156160/128256), FastEthernet0/0.1
P 172.25.25.1/32, 1 successors, FD is 128256
        via Connected, Loopback0
P 172.25.25.2/32, 1 successors, FD is 2297856
        via 172.25.2.2 (2297856/128256), Serial0/0.2
P 172.25.1.0/24, 1 successors, FD is 28160
        via Connected, FastEthernet0/0.1
P 172.25.2.0/30, 1 successors, FD is 2169856
        via Connected, Serial0/0.2
P 172.22.1.0/24, 1 successors, FD is 28160
```

via Connected, FastEthernet0/1

Router1#

第八章 OSPF

8.1. 配置 OSPF

提问 在网络中启用 OSPF

回答

Router5#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router5(config)#**router ospf *87***

Router5(config-router)#**network *0.0.0.0 255.255.255.255* area *0***

Router5(config-router)#**exit**

Router5(config)#**end**

Router5#

注释 这里 OSPF 的进程号是本地使用，不需要像 EIGRP 一样整个网络保持一致。在 12.3(11)T 以后有一个专门的命令来指定端口加入 OSPF 区域，而不需要用 network 的命令

Router9#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router9(config)#**router ospf *87***

Router9(config-router)#**exit**

Router9(config)#**interface *FastEthernet0/0***

Router9(config-if)#**ip address *172.18.5.9 255.255.255.0***

Router9(config-if)#**ip ospf *87* area *10***

Router9(config-if)#**exit**

Router9(config)#**end**

Router9#

8.2. 路由过滤

提问 进行路由过滤，只允许 OSPF 宣告特定路由进入路由表

回答

入方向

Router5#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router5(config)#**access-list *1* deny *172.20.10.0***

Router5(config)#**access-list *1* permit any**

Router5(config)#**router ospf *87***

Router5(config-router)#**distribute-list *1* in *Ethernet0/0***

Router5(config-router)#**exit**

Router5(config)#**end**

Router5#

注释 根据 OSPF 的机制，所有区域内的路由器 LSA 数据库内容必须保持一致，所以正常情况下不能对出方向进行过滤，入方向过滤也是防止其进入路由表，在本地的 LSA 数据库还是有此路由。当然如果确实需要对出方向进行过滤就必须对出方向所有的 LSA 进行过滤，这样会导致下游路由器的 LSA 数据库不完整，一般不推荐使用。

点对多点链路出方向过滤

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**router ospf** ***87***

Router1(config-router)#**neighbor** ***192.168.1.3*** **database-filter all out**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

广播，点到点链路出方向过滤

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface** ***Serial0/0***

Router1(config-if)#**encapsulation frame-relay**

Router1(config-if)#**exit**

Router1(config)#**interface** ***Serial0/0.10*** **multipoint**

Router1(config-subif)#**ip address** ***192.168.1.1 255.255.255.0***

Router1(config-subif)#**ip ospf network broadcast**

Router1(config-subif)#**ip ospf database-filter all out**

Router1(config-subif)#**frame-relay map ip** ***192.168.1.3 101*** **broadcast**

Router1(config-subif)#**frame-relay map ip** ***192.168.1.5 109*** **broadcast**

Router1(config-subif)#**exit**

Router1(config)#**router ospf** ***1***

Router1(config-router)#**network** ***0.0.0.0 255.255.255.255*** **area** ***10***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

8.3. 调整 OSPF 代价值

提问 调整 OSPF 链路的代价值

回答

全局调整

Router5#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router5(config)#**router ospf *87***

Router5(config-router)#**auto-cost reference-bandwidth *1000***

Router5(config-router)#**exit**

Router5(config)#**end**

Router5#

接口调整

Router5#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router5(config)#**interface *Ethernet0***

Router5(config-if)#**ip ospf cost *31***

Router5(config-if)# **exit**

Router5(config)#**end**

Router5#

注释 无

8.4. 宣告缺省路由到 OSPF

提问 宣告缺省路由到 OSPF 网络

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip route** ***0.0.0.0 0.0.0.0 172.25.1.1***

Router1(config)#**router ospf** ***55***

Router1(config-router)#**default-information originate metric** ***30*** **metric-type** ***1***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 在这里不能使用再发布静态路由的命令来发布缺省路由

8.5. 再发布静态路由到 OSPF

提问 宣告一条或者多条静态路由到 OSPF

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip route** ***192.168.10.0 255.255.255.0 172.22.1.4***

Router1(config)#**ip route** ***172.24.1.0 255.255.255.0 172.22.1.4***

Router1(config)#**ip route** ***10.100.1.0 255.255.255.0 172.22.1.4***

Router1(config)#**router ospf** ***55***

Router1(config-router)#**redistribute static**

% Only classful networks will be redistributed

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 根据上面的命令提示可以看到缺省情况下 OSPF 只再发布有类的路由，所以按照例子上虽然三条静态路由但是只有 192.168.10.0/24 是有类路由，能够发布出去，其它两个就不行。这时候就需要配置 **redistribute static subnets** 命令来发布子网，当然也可以添加 metric 等选项

8.6. 再发布外部路由到 OSPF

提问 再发布其它路由协议的路由信息到 OSPF

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**router ospf *55***

Router1(config-router)#**redistribute eigrp *11* subnets**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

在 12.3(2)T 以后增加了下面的命令对再发布过来的条目做了限制

Router1(config-router)#**redistribute maximum-prefix *1000 80***

注释 这里还是要注意 subnet 的参数。对于最后一个条目限制的命令，第一个 1000 是路由条目数，第二个 80 是百分比

8.7. DR 选举

提问 对 DR 选举做人为控制

回答

Router5#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router5(config)#**interface *Ethernet0***

Router5(config-if)#**ip ospf priority *10***

Router5(config-if)#**exit**

Router5(config)#**end**

Router5#

注释 DR 选举人工控制最重要的两种情况是 MOSPF 和 NBMA 网络。在 MOSPF 网络中，MOSPF 的 DR 和正常 OSPF 的 DR 是相同的，而如果 DR 不是一个 MOSPF 的路由器那么所有组播的路由就不能转发，思科路由器是不支持 MOPSF 的，所以在这种情况下必须使用 ip ospf priority 0 的命令来禁止其称为 BDR 或者 DR。在 NBMA 的网络中要将 DR 设置在 Hub 路由器上。还有一个重要的问题是 DR 是不能强占的，如果网络中已经有了 DR，这时即使新加入的路由器有更高的优先级他也不能称为 DR，必须等待现在的 DR 出了问题才可以重新选举为 DR。

8.8. 设置 OSPF RID

提问 人工设定路由器的 Router ID

回答

一种是 Loopback 地址方式

Router5#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router5(config)#**interface *Loopback0***

Router5(config-if)#**ip address *172.25.25.6 255.255.255.255***

Router5(config-if)#**exit**

Router5(config)#**end**

Router5#

一种是 Router ID 命令方式

Router5#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router5(config)#**router ospf *87***

Router5(config-router)#**router-id *172.25.1.7***

Router5(config-if)#**exit**

Router5(config)#**end**

Router5#

注释 缺省会用最大 IP 地址作为 Router ID。Router id 命令后面的 IP 地址可以随意，不需要必须是存在的地址。另外 router id 一旦定下来以后，即使重新修改了地址也不能变更，必须通过 clear

ip ospf process 的方式或者 reload 的方式来改变

8.9.   启用 OSPF 鉴权

提问 对邻居关系建立启用鉴权从而保证网络设备的安全性

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface *Serial0/1***

Router1(config-if)#**ip ospf message-digest-key *1* md5 *oreilly***

Router1(config-if)#**exit**

Router1(config)#**router ospf *55***

Router1(config-router)#**area *2* authentication message-digest**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 注意的是不同厂商的 OPSF MD5 加密认证互联可能会有问题，因为 RFC 没有规范。对于新老密码替换的问题，通过配置新旧两个密码的方式来解决

8.10. 选择合适的区域类型

提问 不同的区域有不同的链路状态数据库，通过不同区域的选择来节省路由器资源和更快收敛

回答

Stubby Area

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**router ospf *55***

Router1(config-router)#**area *100* stub**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

Totally Stubby Area

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**router ospf *55***

Router1(config-router)#**area *100* stub no-summary**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

Not So Stubby Areas (NSSA), 同时生成一条缺省路由

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**router ospf *55***

Router1(config-router)#**area *100* nssa default-information-originate**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

Totally Stubby, Not So Stubby Area.

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**router ospf *55***

Router1(config-router)#**area *100* nssa no-summary**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 这些都是在 ABR 上的配置，对于区域里面其它的路由器就是只有 NSSA 和 stub 的配置没有必要配置是否为 totally stubby。

8.11. 在拨号接口上配置 OSPF

提问 在拨号接口上启用 OSPF，但又不想让 OSPF 的协议数据一直保持拨号链路处于激活状态

回答

下面例子是 R4 只能拨号到 R1

Router4#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router4(config)#**username *Router1* password 0 cisco**

Router4(config)#**interface *BRI0***

Router4(config-if)#**ip address *192.168.15.4 255.255.255.0***

Router4(config-if)#**encapsulation ppp**

Router4(config-if)#**ip ospf demand-circuit**

Router4(config-if)#**dialer map ip *192.168.15.1* broadcast *4165550000***

Router4(config-if)#**dialer-group *1***

Router4(config-if)#**isdn switch-type basic-ni**

Router4(config-if)#**isdn spid1 *416555001000 4165550010***

Router4(config-if)#**isdn spid2 *416555001100 4165550011***

Router4(config-if)#**ppp authentication chap**

Router4(config-if)#**ppp multilink**

Router4(config-if)#**exit**

Router4(config)#**dialer-list *1* protocol ip permit**

Router4(config)#**router ospf** ***87***

Router4(config-router)#**network** ***192.168.15.0 0.0.0.255*** **area** ***10***

Router4(config-router)#**exit**

Router4(config)#**end**

Router4#

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**username** ***Router4*** **password 0** ***cisco***

Router1(config)#**interface** ***BRI0/0***

Router1(config-if)#**ip address** ***192.168.15.1 255.255.255.0***

Router1(config-if)#**encapsulation ppp**

Router1(config-if)#**dialer-group** ***1***

Router1(config-if)#**isdn switch-type basic-ni**

Router1(config-if)#**isdn spid1** ***416555000000 4165550000***

Router1(config-if)#**isdn spid2** ***416555000100 4165550001***

Router1(config-if)#**ppp authentication chap**

Router1(config-if)#**ppp multilink**

Router1(config-if)#**exit**

Router1(config)#**dialer-list** ***1*** **protocol ip permit**

Router1(config)#**router ospf** ***87***

Router1(config-router)#**network** ***192.168.15.0 0.0.0.255*** **area** ***10***

Router1(config-router)#**exit**

```
Router1(config)#end
Router1#
```

注释 使用 *ip ospf demand-circuit* 的命令可以保持邻居关系一直是 FULL 状态，而不管链路是否激活

8.12. 路由汇总

提问 减少路由表大小

回答

```
Router1#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router1(config)#router ospf 55
Router1(config-router)#area 100 range 172.20.0.0 255.255.0.0
Router1(config-router)#area 0 range 172.25.0.0 255.255.0.0
Router1(config-router)#area 2 range 10.0.0.0 255.0.0.0
Router1(config-router)#exit
Router1(config)#end
Router1#
```

注释 OSPF 的路由汇总只能配置在 ABR 上。生成的汇总路由代价值缺省情况下和子网路由中最小的一致，也就是说汇总路由的稳定状态和代价值最小的那个路由条目相关，这也是 RFC1583 上的定义，在新的 RFC 中定义了汇总路由代价值和最大的那个路由条目相关，所以一定要确定所有路由器采用相同的计算方法，思科缺省使用 RFC1583 的方法，禁用可以使用 **no compatible rfc1583**。在 ABR 上启用汇总以后会自动生成一条汇总路由的丢弃路由（12.1(6)）来避免路由回环

8.13. 在特定端口禁用 OSPF

提问 禁止某个端口参与 OSPF

回答

Router3#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router3(config)#**router ospf *44***

Router3(config-router)#**network *0.0.0.0 255.255.255.255* area *100***

Router3(config-router)#**passive-interface *Ethernet0***

Router3(config-router)#**exit**

Router3(config)#**end**

Router3#

注释 OSPF 也是通过配置被动接口的方式来不生成邻居关系从而避免参与 OSPF。当然也可以通过不在 network 命令中包含此端口来禁止，下面就是另外一种很好的配置方法，network 了所有接口，但是缺省所有端口是被动接口，对于需要的接口再使用 no 的命令才参与 OSPF：

Router3(config)#**router ospf *44***

Router3(config-router)#**network *0.0.0.0 255.255.255.255* area *100***

Router3(config-router)#**passive-interface default**

Router3(config-router)#**no passive-interface *Ethernet0***

Router3(config-router)#**exit**

Router3(config)#**end**

Router3#

8.14. 修改接口的网络类型

提问 修改某个端口缺省的网络类型

回答

Router9#**configure terminal**

Enter configuration commands, one per line.　End with CNTL/Z.

Router9(config)#**interface *FastEthernet0/0***

Router9(config-if)#**ip ospf network *?***

broadcast　　　　　　Specify OSPF broadcast multi-access network

non-broadcast　　　　Specify OSPF NBMA network

point-to-multipoint　Specify OSPF point-to-multipoint network

point-to-point　　　　Specify OSPF point-to-point network

Router9(config-if)#

注释 上述四个关键词主要定义媒介是否支持广播或者组播数据包，是否需要选举 DR。对于 Broadcast 网络，支持组播，DR 可以自动选择，不需要配置。对于 nonbroadcast 网络，不支持组播，必须人工使用 neighbor 命令配置邻居关系。对于 point-to-multipoint 网络，不需要 DR 选举，也不需要 neighbor 命令，这时候需要注意的是 framerelay 配置中要允许 broadcast：

Router9(config)#**interface *Serial0/0***

Router9(config-if)#**ip address *192.168.10.9 255.255.255.0***

Router9(config-if)#**encapsulation frame-relay**

Router9(config-if)#**frame-relay map ip *192.168.10.2 123* broadcast**

Router9(config-if)#**ip ospf network point-to-multipoint**

Router9(config-if)#**exit**

Router9(config)#**router ospf *1***

Router9(config-router)#**network *192.168.10.0 0.0.0.255* area *0***

Router9(config-router)#**exit**

否则必须配置 neighbor

Router9(config)#**interface *Serial0/0***

Router9(config-if)#**ip address *192.168.10.9 255.255.255.0***

Router9(config-if)#**encapsulation frame-relay**

Router9(config-if)#**frame-relay map ip *192.168.10.2 123***

Router9(config-if)#**ip ospf network point-to-multipoint non-broadcast**

Router9(config-if)#**exit**

Router9(config)#**router ospf *1***

Router9(config-router)#**network *192.168.10.0 0.0.0.255* area *0***

Router9(config-router)#**neighbor *192.168.10.2***

Router9(config-router)#**exit**

最后一种 point-to-point 网络不需要 DR，但必须支持组播来建立邻居，否则需要配置 neighbor 命令。

还有一个特殊的回环地址，缺省情况 OSPF 会宣告回环地址为/32 的网络，但是你可以在回环接口上配置其为 **ip ospf network point-to-point**，来强制他宣告正确的网络掩码

8.15. 路由标签

提问 对特定的路由打标签避免互相再发布出现路由回环

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**router ospf *55***

Router1(config-router)#**redistribute eigrp *11* metric-type *1* subnets tag *67***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 无

8.16. 记录 OSPF 邻居状态变化

提问 记录 OSPF 邻居状态变化信息

回答

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**router ospf *12***

Router2(config-router)#**log-adjacency-changes**

Router2(config-router)#**exit**

Router2(config)#**end**

Router2#

注释 12.1 后对上面命令增加了 detail 参数可以看到更多邻居状态变化的信息

8.17. OSPF 定时器

提问 调整定时器，加快收敛

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *Serial0/1***

Router1(config-if)#**ip ospf hello-interval *5***

Router1(config-if)#**ip ospf dead-interval *20***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 要保证和此端口相连的设备采用相同的定时器值，否则邻居关系不能建立

8.18. 减少 OSPF 协议流量

提问 在稳定的网络要不需要 LSA 的过多数据包传递

回答

Router9#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router9(config)#**interface *Serial0/0***

Router9(config-if)#**ip address *192.168.10.9 255.255.255.0***

Router9(config-if)#**ip ospf flood-reduction**

Router9(config-if)#**exit**

Router9(config)#**end**

Router9#

注释 正常情况下 OSPF 会每隔一小时进行所有的 LSA 泛洪，在稳定网络里面一般不需要，所以通过这种方式设定 LSA 的 DoNotAge 位，避免过多流量

8.19. OSPF 虚拟链路

提问 把两个分开的路由器通过虚拟链路的方式相连

回答

Router9#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router9(config)#**router ospf** ***1***

Router9(config-router)#**area** ***10*** **virtual-link** ***10.54.0.1***

Router9(config-router)#**exit**

Router9(config)#**end**

Router9#

注释 通过 *show ip ospf virtual-links* 来验证。需要注意的是这个需要两个路由器都进行配置，IP 地址是对方的 Router ID，要确保这个地址是通的，area 后面跟的是穿越的 Area

8.20. 使用域名查看 OSPF 状态

提问 在 OSPF 的 show 命令中显示设备域名而不是地址

回答

Router3#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router3(config)#**ip ospf name-lookup**

Router3(config)#**end**

Router3#

注释 无

8.21. OSPF 排错

提问 对 OSPF 进行排错

回答

Router3#**debug ip ospf adj**

OSPF adjacency events debugging is on

Router3#

注释 OSPF 排错命令很多，这里只提供了对邻居关系的排错命令，因为邻居是 OSPF 的基础

第九章 BGP

9.1. 配置 BGP

提问 在网络中启用 BGP

回答

Route1 在 AS 65500 中

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface *Serial0***

Router1(config-if)#**ip address *192.168.55.6 255.255.255.252***

Router1(config-if)#**exit**

Router1(config)#**router bgp *65500***

Router1(config-router)#**network *192.168.1.0***

Router1(config-router)#**neighbor *192.168.55.5* remote-as *65501***

Router1(config-router)#**no synchronization**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

Router2 在 AS 65501 中

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

```
Router2(config)#interface Serial0
Router2(config-if)#ip address 192.168.55.5 255.255.255.252
Router2(config-if)#exit
Router2(config)#router bgp 65501
Router2(config-router)#network 172.25.17.0 mask 255.255.255.0
Router2(config-router)#neighbor 192.168.55.6 remote-as 65500
Router2(config-router)#no synchronization
Router2(config-router)#exit
Router2(config)#end
Router2#
```

注释 在对 BGP 验证的时候比较有用的命令是

```
Router1#show ip bgp summary
BGP router identifier 192.168.99.5, local AS number 65500
BGP table version is 7, main routing table version 7
4 network entries and 4 paths using 484 bytes of memory
2 BGP path attribute entries using 196 bytes of memory
BGP activity 11/7 prefixes, 11/7 paths

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
192.168.55.5    4 65501      17      18        7    0    0 00:12:38        2
172.25.2.2      4 65531     527     526        0    0    0 21:05:23 Active
Router1#
```

需要注意的是理想状态是 State 里面是数字，尽管是 Active 也不代表是配置正常，反而有可能是配置出现错误。通过 **neighbor *172.20.1.2* update-source *Loopback0*** 命令来限制 BGP 数据包源地址为回环地址，但要确保此地址的连通性

9.2. 使用 EBGP MULTIHOP

提问 配置外部 BGP，但是不是直连的路由器

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip route *172.20.1.2 255.255.255.255 192.168.1.5 2***

Router1(config)#**router bgp *65500***

Router1(config-router)#**neighbor *172.20.1.2* remote-as *65530***

Router1(config-router)#**neighbor *172.20.1.2* update-source *Loopback0***

Router1(config-router)#**neighbor *172.20.1.2* ebgp-multihop *3***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 缺省情况下 eBGP 的路由器必须是直连的，如果不是直连的就需要使用此命令。一种说法是此跳数越小越好，但是 RFC 3682 说为了安全还是越大越好，思科在 12.3(7)T 后也采用了这个建议，使用了 **neighbor *192.168.55.5* ttl-security hops *1*** 命令，此命令会丢弃所有 TTL 小于 255-1＝254 的 BGP 数据包，这时候如果对端 eBGP 邻居不支持此特性就必须使用下面的命令来配置 **neighbor *192.168.55.6* ebgp-multihop *255***

9.3. 调整 NEXT-HOP 属性值

提问 在 iBGP 之间宣告路由时候修改下一跳属性值，使其指向内部 AS 的地址

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**router bgp *65500***

Router1(config-router)#**neighbor *192.168.1.6* remote-as *65500***

Router1(config-router)#**neighbor *192.168.1.6* next-hop-self**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 正常情况下 iBGP 之间下一跳属性值是不会修改的，只会在 eBGP 时会进行修改，而此地址会指向 eBGP 邻居的地址，而往往内部 AS 的路由器没有到达此地址的路由。

9.4. 连接两个 ISPS

提问 一台路由器连接两个 ISP，保证网络冗余

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface *Serial0***

Router1(config-if)#**description *connection to ISP #1, ASN 65510***

Router1(config-if)#**ip address *192.168.1.6 255.255.255.252***

Router1(config-if)#**exit**

Router1(config)#**interface *Serial1***

Router1(config-if)#**description *connection to ISP #2, ASN 65520***

Router1(config-if)#**ip address *192.168.2.6 255.255.255.252***

Router1(config-if)#**exit**

Router1(config)#**interface *Ethernet0***

Router1(config-if)#**description *connection to internal network, ASN 65500***

Router1(config-if)#**ip address *172.18.5.2 255.255.255.0***

Router1(config-if)#**exit**

Router1(config)#**router bgp *65500***

Router1(config-router)#**network *172.18.5.0* mask *255.255.255.0***

Router1(config-router)#**neighbor *192.168.1.5* remote-as *65510***

Router1(config-router)#**neighbor *192.168.2.5* remote-as *65520***

Router1(config-router)#**no synchronization**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 注意此配置不是最佳配置，可能导致内部 AS 称为两个 ISP 的 transit AS，同时导致自己路由器接收过多路由

9.5. 两台路由器分别连接两个 ISP

提问 内部 AS 有两台路由器，分别连两个 ISP 保证网络冗余

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *Serial0***

Router1(config-if)#**description *connection to ISP #1, ASN 65510***

Router1(config-if)#**ip address *192.168.1.6 255.255.255.252***

Router1(config-if)#**exit**

Router1(config)#**interface *Ethernet0***

Router1(config-if)#**description *connection to internal network, ASN 65500***

Router1(config-if)#**ip address *172.18.5.2 255.255.255.0***

Router1(config-if)#**exit**

Router1(config)#**ip as-path access-list *15* permit ^$**

Router1(config)#**router bgp *65500***

Router1(config-router)#**network *172.18.5.0* mask *255.255.255.0***

Router1(config-router)#**neighbor *172.18.5.3* remote-as *65500***

Router1(config-router)#**neighbor *172.18.5.3* next-hop-self**

Router1(config-router)#**neighbor *192.168.1.5* remote-as *65510***

Router1(config-router)#**neighbor *192.168.1.5* filter-list *15* out**

Router1(config-router)#**no synchronization**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**interface *Serial1***

Router2(config-if)#**description *connection to ISP #2, ASN 65520***

Router2(config-if)#**ip address *192.168.2.6 255.255.255.252***

Router2(config-if)#**exit**

Router2(config)#**interface *Ethernet0***

Router2(config-if)#**description *connection to internal network, ASN 65500***

Router2(config-if)#**ip address *172.18.5.3 255.255.255.0***

Router2(config-if)#**exit**

Router2(config)#**ip as-path access-list *15* permit ^$**

Router2(config)#**router bgp *65500***

Router2(config-router)#**network *172.18.5.0* mask *255.255.255.0***

Router2(config-router)#**neighbor *192.168.2.5* remote-as *65520***

Router2(config-router)#**neighbor *192.168.2.5* filter-list *15* out**

Router2(config-router)#**neighbor *172.18.5.2* remote-as *65500***

Router2(config-router)#**neighbor *172.18.5.2* next-hop-self**

Router2(config-router)#**no synchronization**

Router2(config-router)#**exit**

Router2(config)#**end**

Router2#

注释 无

9.6. 限制向 BGP 对端的网络宣告

提问 限制特定的路由公告给对端的 AS

回答

有三种方法，第一种是扩展 ACL

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**access-list *105* deny ip host *172.25.0.0* host *255.255.0.0***

Router1(config)#**access-list *105* permit ip any any**

Router1(config)#**route-map *ACL-RT-FILTER* permit *10***

Router1(config-route-map)#**match ip address *105***

Router1(config-route-map)#**exit**

Router1(config)#**route-map *ACL-RT-FILTER* deny *20***

Router1(config-route-map)#**exit**

Router1(config)#**router bgp *65500***

Router1(config-router)#**neighbor *192.168.1.5* remote-as *65510***

Router1(config-router)#**neighbor *192.168.1.5* route-map *ACL-RT-FILTER* in**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

第二种是使用 *distribute-list*:

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**access-list *106* deny ip host *172.25.0.0* host *255.255.0.0***

Router1(config)#**access-list *106* permit ip any any**

Router1(config)#**router bgp *65500***

Router1(config-router)#**neighbor *192.168.1.5* remote-as *65510***

Router1(config-router)#**neighbor *192.168.1.5* distribute-list *106* in**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

第三种也是最常用的是使用 prefix lists

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip prefix-list *PREFIX-FILTER* seq *10* deny *172.25.0.0/16***

Router1(config)#**ip prefix-list *PREFIX-FILTER* seq *20* permit *0.0.0.0/0* le *32***

Router1(config)#**router bgp *65500***

Router1(config-router)#**neighbor *192.168.1.5* remote-as *65510***

Router1(config-router)#**neighbor *192.168.1.5* prefix-list *PREFIX-FILTER* in**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 前两种使用的扩展 ACL 比较奇特，第一个 host 是子网，第二个 host 是子网掩码，而不是传统目的地址，所以 host 172.25.0.0 host 255.255.0.0 就代表网络 172.25.0.0/16，如果用正常的 ACL 就实现不了对无类网络的控制。所以推荐使用第三种方式 prefixlist，此列表支持序列号，可以帮助你修改和插入新的条目 ge 是大于，le 是小于，控制子网掩码 permit 0.0.0.0/0 le 32 就是变相的 permit any

9.7. 调整 LOCAL PREFERENCE 属性值

提问 调整 Local Preference 属性值来控制路由选择

回答

第一种全局

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**router bgp *65500***

Router1(config-router)#**bgp default local-preference *200***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

第二种使用 route map 控制

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip prefix-list *LOW_LP_PREFIXES* seq *10* permit *172.22.0.0/16***

Router1(config)#**route-map *LOCALPREF* permit *10***

Router1(config-route-map)#**match ip address prefix-list *LOW_LP_PREFIXES***

Router1(config-route-map)#**set local-preference *50***

Router1(config-route-map)#**exit**

Router1(config)#**route-map *LOCALPREF* permit *20***

Router1(config-route-map)#**exit**

Router1(config)#**router bgp *65500***

Router1(config-router)#**neighbor *192.168.1.5* remote-as *65510***

Router1(config-router)#**neighbor *192.168.1.5* route-map *LOCALPREF* in**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 此 local preference 属性值只在内部 AS 有用，选路级别高于 AS Path。此值越大优先级越高，缺省值为 100。Show ip bgp 命令可以看到各个路由的 local preference 属性值

9.8. 负载均衡

提问 在 BGP 邻居之间的多链路上负载均衡流量

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**router bgp *65500***

Router1(config-router)#**maximum-paths *4***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 正常情况下 BGP 选路策略会保证只有一条路径，通过此命令可以增加到 4 条，不过要确保所有属性值相同，包括 MED 属性。同时注意此负载均衡只针对出流量而不适合入流量

9.9. 在 AS PATH 属性值中清除私有 ASNS

提问 避免内网中的私有 ASN 传播到互联网

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *Serial0***

Router1(config-if)#**description *connection to ISP #1, ASN 1***

Router1(config-if)#**ip address *192.168.1.6 255.255.255.252***

Router1(config-if)#**exit**

Router1(config)#**interface *Serial1***

Router1(config-if)#**description *connection to private network, ASN 65500***

Router1(config-if)#**ip address *192.168.5.1 255.255.255.252***

Router1(config-if)#**exit**

Router1(config)#**router bgp *2***

Router1(config-router)#**neighbor *192.168.5.2* remote-as *65500***

Router1(config-router)#**neighbor *192.168.1.5* remote-as *1***

Router1(config-router)#**neighbor *192.168.1.5* remove-private-AS**

Router1(config-router)#**no synchronization**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 注意此命令是不能删除那些在公共 ASN 之间的私有 ASN

9.10. 基于 AS PATH 属性值的路由过滤

提问 基于接收或者发送路由的 AS Path 属性值进行路由过滤

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip as-path access-list *15* permit *^65501$***

Router1(config)#**ip as-path access-list *25* permit *_65530_***

Router1(config)#**ip as-path access-list *25* deny *_65531$***

Router1(config)#**ip as-path access-list *25* permit *.****

Router1(config)#**router bgp *65500***

Router1(config-router)#**neighbor *192.168.1.5* remote-as *65510***

Router1(config-router)#**neighbor *192.168.1.5* filter-list *15* in**

Router1(config-router)#**neighbor *192.168.2.5* remote-as *65520***

Router1(config-router)#**neighbor *192.168.2.5* filter-list *25* out**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 正则表达式过滤

9.11. 减少接收到的路由表大小

提问 通过汇总接收到路由的方式来减少所接收的路由表大小

回答

通过缺省路由的方式来过滤到过多的外部路由

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip route *0.0.0.0 0.0.0.0 192.168.101.0 1***

Router1(config)#**ip route *0.0.0.0 0.0.0.0 192.168.102.0 2***

Router1(config)#**ip prefix-list *CREATE-DEFAULT* seq *10* permit *192.168.101.0/24***

Router1(config)#**ip prefix-list *CREATE-DEFAULT* seq *20* permit *192.168.102.0/24***

Router1(config)#**router bgp *65500***

Router1(config-router)#**neighbor *192.168.1.5* remote-as *65520***

Router1(config-router)#**neighbor *192.168.1.5* prefix-list *CREATE-DEFAULT* in**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 无

9.12. 出方向路由信息汇总

提问 在向下游路由器发送路由表之前进行路由汇总

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**router bgp** 65500

Router1(config-router)#**neighbor** 192.168.1.5 **remote-as** 65520

Router1(config-router)#**auto-summary**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 这是缺省行为，但是是有类的汇总，并且只能针对再分发过来的路由，不能适用于 network 命令配置的路由。思科使用了如下命令对出方向路由进行汇总

Router3(config)#**router bgp** ***65530***

Router3(config-router)#**aggregate-address** ***172.20.0.0 255.252.0.0*** **summary-only**

Summaryonly 选项只发布汇总路由，去掉后会发送汇总路由和子网路由，而为了避免回环建议添加 as-set 选项

9.13. 在 AS PATH 属性值中添加更多 ASN

提问 通过增加 AS Path 属性中 ASN 的数目来影响 BGP 选路

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip as-path access-list** ***15*** **permit ^$**

Router1(config)#**route-map** ***PREPEND*** **permit** ***10***

Router1(config-route-map)#**match as-path** ***15***

Router1(config-route-map)#**set as-path prepend** ***65500 65500 65500***

Router1(config-route-map)#**exit**

Router1(config)#**route-map** ***PREPEND*** **permit** ***20***

Router1(config-route-map)#**exit**

Router1(config)#**router bgp** ***65500***

Router1(config-router)#**neighbor** ***192.168.1.5*** **remote-as** ***65510***

Router1(config-router)#**neighbor** ***192.168.1.5*** **route-map** ***PREPEND*** **out**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 通过这种方式来影响入流量

9.14. 再发布路由到 BGP

提问 IGP 和 BGP 之间的再分发

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**router ospf *100***

Router1(config-router)#**network *172.26.0.0 0.0.255.255* area *0***

Router1(config-router)#**redistribute bgp *65500* metric *500* subnets**

Router1(config-router)#**exit**

Router1(config)#**router bgp *65500***

Router1(config-router)#**neighbor *192.168.1.5* remote-as *65520***

Router1(config-router)#**network *172.26.0.0***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

Router2(config)#**route-map *REDIST* permit *5***

Router2(config-route-map)#**match tag *123***

Router2(config-route-map)#**exit**

Router2(config)#**route-map *REDIST* deny *10***

Router2(config-route-map)#**match route-type external**

Router2(config-route-map)#**exit**

Router2(config)#**route-map *REDIST* permit *20***

Router2(config-route-map)#**exit**

Router2(config)#**router bgp *65520***

Router2(config-router)#**redistribute eigrp *99* route-map *REDIST* metric *500***

注释 无

9.15. 使用 PEER GROUPS

提问 使用组的形式来简化对多个相同属性邻居的配置

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**router bgp *65500***

Router1(config-router)#**neighbor *EBGP-PEERS* peer-group**

Router1(config-router)#**neighbor *EBGP-PEERS* prefix-list *PRE-RTFILTER* in**

Router1(config-router)#**neighbor *EBGP-PEERS* filter-list *15* out**

Router1(config-router)#**neighbor *192.168.1.5* remote-as *65520***

Router1(config-router)#**neighbor *192.168.1.5* peer-group *EBGP-PEERS***

Router1(config-router)#**neighbor *192.168.1.9* remote-as *65521***

Router1(config-router)#**neighbor *192.168.1.9* peer-group *EBGP-PEERS***

Router1(config-router)#**neighbor *192.168.1.13* remote-as *65522***

Router1(config-router)#**neighbor *192.168.1.13* peer-group *EBGP-PEERS***

Router1(config-router)#**neighbor *192.168.1.17* remote-as *65523***

Router1(config-router)#**neighbor *192.168.1.17* peer-group *EBGP-PEERS***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 当然也可以针对 iBGP 邻居

Router1(config)#**router bgp *6550***

Router1(config-router)#**neighbor *IBGP-PEERS* peer-group**

Router1(config-router)#**neighbor *IBGP-PEERS* update-source *Loopback0***

Router1(config-router)#**neighbor *IBGP-PEERS* route-reflector-client**

Router1(config-router)#**neighbor *192.168.101.5* remote-as *65500***

Router1(config-router)#**neighbor *192.168.101.5* peer-group *IBGP-PEERS***

Router1(config-router)#**neighbor *192.168.101.9* remote-as *65500***

Router1(config-router)#**neighbor *192.168.101.9* peer-group *IBGP-PEERS***

9.16. BGP 邻居认证

提问 使用认证增加安全性

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**router bgp *65500***

Router1(config-router)#**neighbor *192.168.55.5* remote-as *65501***

Router1(config-router)#**neighbor *192.168.55.5* password *password-1234***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 无

9.17. 使用 BGP COMMUNITIES

提问 使用 BGP Communities 来对路由进行控制

回答

首先要通过 route map 的方式针对邻居设定希望的 Communities 值

Router3#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router3(config)#**ip prefix-list *10.101/16* seq *5* permit *10.101.0.0/16***

Router3(config)#**ip prefix-list *10.102/16* seq *5* permit *10.102.0.0/16***

Router3(config)#**ip prefix-list *10.103/16* seq *5* permit *10.103.0.0/16***

Router3(config)#**ip prefix-list *10.104/16* seq *5* permit *10.104.0.0/16***

Router3(config)#**ip prefix-list *10.105/16* seq *5* permit *10.105.0.0/16***

Router3(config)#**route-map *APPLY_COMMUNITY_A* permit *10***

Router3(config-route-map)#**match ip address prefix-list *10.101/16***

Router3(config-route-map)#**set community *no-advertise***

Router3(config-route-map)#**exit**

Router3(config)#**route-map *APPLY_COMMUNITY_A* permit *20***

Router3(config-route-map)#**match ip address prefix-list** ***10.102/16***

Router3(config-route-map)#**set community** ***no-export***

Router3(config-route-map)#**exit**

Router3(config)#**route-map** ***APPLY_COMMUNITY_A*** **permit** ***30***

Router3(config-route-map)#**match ip address prefix-list** ***10.103/16***

Router3(config-route-map)#**set community** ***local-AS***

Router3(config-route-map)#**exit**

Router3(config)#**route-map** ***APPLY_COMMUNITY_A*** **permit** ***40***

Router3(config-route-map)#**match ip address prefix-list** ***10.104/16***

Router3(config-route-map)#**set community** ***internet***

Router3(config-route-map)#**exit**

Router3(config)#**route-map** ***APPLY_COMMUNITY_A*** **permit** ***50***

Router3(config-route-map)#**match ip address prefix-list** ***10.105/16***

Router3(config-route-map)#**set community** ***4293328976***

Router3(config-route-map)#**exit**

Router3(config)#**route-map** ***APPLY_COMMUNITY_A*** **permit** ***100***

Router3(config-route-map)#**exit**

Router3(config)#**router bgp** ***65500***

Router3(config-router)#**no synchronization**

Router3(config-router)#**neighbor** ***172.18.5.3*** **remote-as** ***65500***

Router3(config-router)#**neighbor** ***172.18.5.3*** **next-hop-self**

Router3(config-router)#**neighbor** ***172.18.5.3*** **send-community both**

Router3(config-router)#**neighbor *172.18.5.10* remote-as *65500***

Router3(config-router)#**neighbor *172.18.5.10* next-hop-self**

Router3(config-router)#**neighbor *172.18.5.10* send-community both**

Router3(config-router)#**neighbor *192.168.1.9* remote-as *65520***

Router3(config-router)#**neighbor *192.168.1.9* send-community both**

Router3(config-router)#**neighbor *192.168.1.9* route-map *APPLY_COMMUNITY_A* in**

Router3(config-router)#**exit**

Router3(config)#end

Router3#

在下游路由器上配置命令使其可以分发此 Community 值

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**router bgp *65500***

Router2(config-router)#**no synchronization**

Router2(config-router)#**neighbor *172.18.5.4* remote-as *65500***

Router2(config-router)#**neighbor *172.18.5.4* send-community both**

Router2(config-router)#**neighbor *172.18.5.10* remote-as *65500***

Router2(config-router)#**neighbor *172.18.5.10* send-community both**

Router2(config-router)#**no auto-summary**

Router2(config-router)#**exit**

Router2(config)#**end**

Router2#

注释 通过定义 local-as,no-advertise,no-export,internet 四种不同 community 属性值的方式来限制路由公告的范围

9.18. 使用 BGP 路由反射器

提问 通过路由反射器的方式来简化 iBGP 邻居关系

回答

只要针对三种不同角色路由器的配置

Router1 是 Client Peer:

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *Ethernet0/0***

Router1(config-if)#**ip address *172.18.5.2 255.255.255.0***

Router1(config-if)#**exit**

Router1(config)#**interface *Serial0/0***

Router1(config-if)#**ip address *192.168.1.6 255.255.255.252***

Router1(config-if)#**exit**

Router1(config)#**interface *Loopback0***

Router1(config-if)#**ip address *172.18.6.1 255.255.255.255***

Router1(config-if)#**exit**

Router1(config)#**router bgp *65500***

Router1(config-router)#**no synchronization**

Router1(config-router)#**neighbor *172.18.6.2* remote-as *65500***

Router1(config-router)#**neighbor *172.18.6.2* next-hop-self**

Router1(config-router)#**neighbor** ***172.18.6.2*** **update-source** ***Loopback0***

Router1(config-router)#**neighbor** ***192.168.1.5*** **remote-as** ***65510***

Router1(config-router)#**exit**

Router1(config)#**ip route** ***172.18.6.2 255.255.255.255 172.18.5.3***

Router1(config)#**ip route** ***172.18.6.3 255.255.255.255 172.18.5.4***

Router1(config)#**ip route** ***172.18.6.4 255.255.255.255 172.18.5.10***

Router1(config)#**end**

Router1#

Router4 是 Nonclient Peer:

Router4#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router4(config)#**interface** ***Ethernet0***

Router4(config-if)#**ip address** ***172.18.5.10 255.255.255.0***

Router4(config-if)#**exit**

Router4(config)#**interface** ***Loopback0***

Router4(config-if)#**ip address** ***172.18.6.4 255.255.255.255***

Router4(config-if)#**exit**

Router4(config)#**router bgp** ***65500***

Router4(config-router)#**no synchronization**

Router4(config-router)#**neighbor** ***172.18.6.2*** **remote-as** ***65500***

Router4(config-router)#**neighbor** ***172.18.6.2*** **update-source** ***Loopback0***

Router4(config-router)#**exit**

Router4(config)#**ip route *172.18.6.1 255.255.255.255 172.18.5.2***

Router4(config)#**ip route *172.18.6.2 255.255.255.255 172.18.5.3***

Router4(config)#**ip route *172.18.6.3 255.255.255.255 172.18.5.4***

Router4(config)#**end**

Router4#

R2 是 Route Reflector

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**interface *FastEthernet0/0***

Router2(config-if)#**ip address *172.18.5.3 255.255.255.0***

Router2(config-if)#**exit**

Router2(config)#**interface *Loopback0***

Router2(config-if)#**ip address *172.18.6.2 255.255.255.255***

Router2(config-if)#**exit**

Router2(config)#**router bgp *65500***

Router2(config-router)#**no synchronization**

Router2(config-router)#**neighbor *172.18.6.1* remote-as *65500***

Router2(config-router)#**neighbor *172.18.6.1* route-reflector-client**

Router2(config-router)#**neighbor *172.18.6.1* update-source *Loopback0***

Router2(config-router)#**neighbor *172.18.6.3* remote-as *65500***

Router2(config-router)#**neighbor *172.18.6.3* route-reflector-client**

Router2(config-router)#**neighbor *172.18.6.3* update-source *Loopback0***

Router2(config-router)#**neighbor *172.18.6.4* remote-as *65500***

Router2(config-router)#**neighbor *172.18.6.4* update-source *Loopback0***

Router2(config-router)#**no auto-summary**

Router2(config-router)#**exit**

Router2(config)#**ip route *172.18.6.1 255.255.255.255 172.18.5.2***

Router2(config)#**ip route *172.18.6.3 255.255.255.255 172.18.5.4***

Router2(config)#**ip route *172.18.6.4 255.255.255.255 172.18.5.10***

Router2(config)#**end**

Router2#

注释 路由反射器是解决要求 iBGP 全互联的问题。不过为了保证冗余性还是要配置多个路由反射器，使用 **bgp cluster-id** ***1234*** 命令来定义 cluster

9.19. 汇总实验

提问 结合前面的方法，重新配置一台路由器两个冗余链路的情况

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *Serial0***

Router1(config-if)#**description *connection to ISP #1, ASN 65510***

Router1(config-if)#**ip address *192.168.1.6 255.255.255.252***

Router1(config-if)#**exit**

Router1(config)#**interface *Serial1***

Router1(config-if)#**description *connection to ISP #2, ASN 65520***

Router1(config-if)#**ip address** ***192.168.2.6 255.255.255.252***

Router1(config-if)#**exit**

Router1(config)#**interface** ***Ethernet0***

Router1(config-if)#**description** ***connection to internal network, ASN 65500***

Router1(config-if)#**ip address** ***172.18.5.2 255.255.255.0***

Router1(config-if)#**exit**

Router1(config)#**ip as-path access-list** ***15*** **permit ^$**

Router1(config)#**ip route** ***0.0.0.0 0.0.0.0 192.168.101.0 1***

Router1(config)#**ip route** ***0.0.0.0 0.0.0.0 192.168.102.0 2***

Router1(config)#**ip prefix-list** ***CREATE-DEFAULT*** **seq** ***10*** **permit** ***192.168.101.0/24***

Router1(config)#**ip prefix-list** ***CREATE-DEFAULT*** **seq** ***20*** **permit** ***192.168.102.0/24***

Router1(config)#**ip prefix-list** ***BLOCK-DEFAULT*** **seq** ***10*** **permit** ***0.0.0.0/0*** **ge** ***1***

Router1(config)#**route-map** ***PREPEND*** **permit** ***10***

Router1(config-route-map)#**set as-path prepend** ***65500 65500***

Router1(config-route-map)#**exit**

Router1(config)#**route-map** ***LOCALPREF*** **permit** ***10***

Router1(config-route-map)#**set local-preference** ***75***

Router1(config-route-map)#**exit**

Router1(config)#**route-map** ***DEFAULT-ROUTE*** **permit** ***10***

Router1(config-route-map)#**match ip address prefix-list** ***CREATE-DEFAULT***

Router1(config-route-map)#**exit**

Router1(config)#**router bgp** ***65500***

Router1(config-router)#**network *172.18.5.0* mask *255.255.255.0***

Router1(config-router)#**neighbor *172.18.5.3* remote-as *65500***

Router1(config-router)#**neighbor *172.18.5.3* password *password_number1***

Router1(config-router)#**neighbor *172.18.5.3* default-origniate route-map *DEFAULT-ROUTE***

Router1(config-router)#**neighbor *192.168.1.5* remote-as *65510***

Router1(config-router)#**neighbor *192.168.1.5* password *password_number2***

Router1(config-router)#**neighbor *192.168.1.5* filter-list *15* out**

Router1(config-router)#**neighbor *192.168.1.5* prefix-list *CREATE-DEFAULT* in**

Router1(config-router)#**neighbor *192.168.1.5* prefix-list *BLOCK-DEFAULT* out**

Router1(config-router)#**neighbor *192.168.2.5* remote-as *65520***

Router1(config-router)#**neighbor *192.168.2.5* password *password_number3***

Router1(config-router)#**neighbor *192.168.2.5* filter-list *15* out**

Router1(config-router)#**neighbor *192.168.2.5* prefix-list *CREATE-DEFAULT* in**

Router1(config-router)#**neighbor *192.168.2.5* prefix-list *BLOCK-DEFAULT* out**

Router1(config-router)#**neighbor *192.168.2.5* route-map *PREPEND* out**

Router1(config-router)#**neighbor *192.168.2.5* route-map *LOCALPREF* in**

Router1(config-router)#**no synchronization**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 无

第十章 帧中继

10.1. 使用点对点子接口的方式配置帧中继

提问 每个 PVC 归属特定子接口的方式来配置帧中继

回答

中心配置

Central#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Central(config)#**interface *Serial0***

Central(config-if)#**description *Frame-Relay host circuit***

Central(config-if)#**no ip address**

Central(config-if)#**encapsulation frame-relay**

Central(config-if)#**exit**

Central(config)#**interface *Serial0.1* point-to-point**

Central(config-subif)#**description *PVC to first branch - DLCI 101***

Central(config-subif)#**ip address *192.168.1.5 255.255.255.252***

Central(config-subif)#**frame-relay interface-dlci *101***

Central(config-fr-dlci)#**exit**

Central(config-subif)#**exit**

Central(config)#**interface *Serial0.2* point-to-point**

Central(config-subif)#**description *PVC to second branch - DLCI 102***

Central(config-subif)#**ip address *192.168.1.9 255.255.255.252***

Central(config-subif)#**frame-relay interface-dlci *102***

Central(config-fr-dlci)#**exit**

Central(config-subif)#**exit**

Central(config)#**end**

Central#

边缘配置

Branch1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Branch1(config)#**interface *Serial0***

Branch1(config-if)#**description *Frame-Relay circuit***

Branch1(config-if)#**no ip address**

Branch1(config-if)#**encapsulation frame-relay**

Branch1(config-if)#**exit**

Branch1(config)#**interface *Serial0.1* point-to-point**

Branch1(config-subif)#**description *PVC to Central host - DLCI 50***

Branch1(config-subif)#**ip address *192.168.1.6 255.255.255.252***

Branch1(config-subif)#**frame-relay interface-dlci *50***

Branch1(config-fr-dlci)#**exit**

Branch1(config-if)#**exit**

Branch1(config)#**end**

Branch1#

注释 点对点子接口方式应该是最简单的一种帧中继配置方式了。对于互联非思科设备时候可能需要人工指定包封装格式为标准的 IETF 格式(RFC1490),可以在接口下配置 **encapsulation frame-relay ietf** 或者在子接口下配置 **frame-relay interface-dlci *101* ietf**。当你启用帧中继的时候路由器会自动激活 Inverse ARP，而通常都是自动配置映射关系，所以我们一般都不需要 **no frame-relay inverse-arp**。还

有要注意的是这里的 **interface *Serial0.1* point-to-point**，后面的子接口模式不能写错，否则需要删除错误的，然后重启才可以更改

10.2. 调整 LMI 选项

提问 在帧中继电路上配置不同的 LMI

回答

Branch1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Branch1(config)#**interface *Serial0***

Branch1(config-if)#**encapsulation frame-relay**

Branch1(config-if)#**frame-relay lmi-type ansi** （**cisco**，**q933a**）

Branch1(config-if)#**exit**

Branch1(config)#**end**

Branch1#

缺省情况下 LMI 的 Keeplive 包每十秒钟发一次，也可以调整此间隔

Branch1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Branch1(config)#**interface *Serial0***

Branch1(config-if)#**encapsulation frame-relay**

Branch1(config-if)#**keepalive *5***

Branch1(config-if)#**exit**

Branch1(config)#**end**

Branch1#

对于不支持 LMI 的网络必须配置路由器宣告自己的 DLCI

Branch1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Branch1(config)#**interface *Serial0***

Branch1(config-if)#**encapsulation frame-relay**

Branch1(config-if)#**frame-relay local-dlci *50***

Branch1(config-if)#**exit**

Branch1(config)#**end**

Branch1#

注释 对于最后不支持 LMI 的例子中建议用 **no keepalive** 来关闭 LMI 的轮询

10.3. 使用 MAP 命令配置

提问 所有的 PVC 共享同一个接口

回答

Central#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Central(config)#**interface *Serial0***

Central(config)#**description *Frame Relay to branches***

Central(config-if)#**ip address *192.168.1.1 255.255.255.0***

Central(config-if)#**encapsulation frame-relay**

Central(config-if)#**frame-relay map ip *192.168.1.10 101***

Central(config-if)#**frame-relay map ip *192.168.1.11 102***

Central(config-if)#**frame-relay map ip *192.168.1.12 103***

Central(config-if)#**exit**

Central(config)#**end**

Central#

注释 在 10.1 中使用了点对点子接口的方式来配置，此小节 MAP 的方式和下节的多点子接口都是类似的实现方法，但是在网管中点对点可以生成各个 PVC 的 trap，而后两种则无法针对每个链路产生告警。同时由于帧中继是 NBMA 网络，所以建议 **frame-relay map ip *192.168.1.10 101* broadcast** 方式来允许广播包的传递

10.4. 使用多点子接口

提问 所有的 PVC 共享同一个接口

回答

Central#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Central(config)#**interface *Serial0.1* multipoint**

Central(config-subif)#**description *Frame Relay to branches***

Central(config-subif)#**ip address *192.168.1.1 255.255.255.0***

Central(config-subif)#**frame-relay interface-dlci *101***

Central(config-subif)#**frame-relay interface-dlci *102***

Central(config-subif)#**frame-relay interface-dlci *103***

Central(config-subif)#**frame-relay interface-dlci *104***

Central(config-subif)#**exit**

Central(config)#**end**

Central#

注释 这种配置方式最大的不同就是不需要配置映射，使用的 Inverse ARP，所以在这种模式下不能禁用反向 ARP。可以通过 show frame-relay map 命令来验证

10.5. 配置帧中继 SVCS

提问 配置路由器使其支持帧中继 SVC

回答

SVC 子接口模式

Central#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Central(config)#**interface *Serial0***

Central(config-if)#**encapsulation frame-relay**

Central(config-if)#**frame-relay lmi-type q933a**

Central(config-if)#**frame-relay svc**

Central(config-if)#**exit**

Central(config)#**interface *Serial0.10* point-to-point**

Central(config-subif)#**ip address *192.168.1.129 255.255.255.252***

Central(config-subif)#**frame-relay interface-dlci *100***

Central(config-subif)#**map-group *SVCMAP***

Central(config-fr-dlci)#**class *SVCclass***

Central(config-fr-dlci)#**exit**

Central(config-subif)# **exit**

Central(config)#**map-list *SVCMAP* source-addr X121 *1234* dest-addr X121 *4321***

Central(config-map-list)#**ip *192.168.55.6* class *SVCclass* ietf**

Central(config-map-list)#**exit**

Central(config)#**map-class frame-relay *SVCclass***

Central(config-map-class)#**frame-relay traffic-rate *56000 128000***

Central(config-map-class)#**exit**

Central(config)#**end**

Central#

SVC 非子接口模式

Central#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Central(config)#**interface *Serial0***

Central(config-if)#**ip address *192.168.55.1 255.255.255.0***

Central(config-if)#**encapsulation frame-relay**

Central(config-if)#**frame-relay lmi-type q933a**

Central(config-if)#**frame-relay svc**

Central(config-if)#**map-group *SVCMAP***

Central(config-if)#**frame-relay interface-dlci *50***

Central(config-fr-dlci)#**class *SVCclass***

Central(config-fr-dlci)#**exit**

Central(config-if)#**exit**

Central(config)#**map-list *SVCMAP* source-addr X121 *1234* dest-addr X121 *4321***

Central(config-map-list)#**ip *192.168.55.6* class *SVCclass* ietf**

Central(config-map-list)#**exit**

Central(config)#**map-class frame-relay *SVCclass***

Central(config-map-class)#**frame-relay traffic-rate *56000 128000***

Central(config-map-class)#**exit**

Central(config)#**end**

Central#

注释 缺省情况下在空闲 120 秒后此 SVC 会被拆除，可以使用 **frame-relay idle-timer** 命令来修改。通过 **show frame-relay svc maplist *SVCMAP*** 来验证。一般网络中都使用 PVC，SVC 用于节省成本，但是增加了复杂性和管理难度，路由器可以自动增加或者删除链路

10.6. 模拟帧中继云

提问 使用一台路由器来模拟帧中继交换机

回答

Cloud#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Cloud(config)#**frame-relay switching**

Cloud(config)#**interface *Serial0***

Cloud(config-if)#**description *Frame-relay connection to Central - DLCI 50***

Cloud(config-if)#**encapsulation frame-relay**

Cloud(config-if)#**clock rate *125000***

Cloud(config-if)#**frame-relay lmi-type *cisco***

Cloud(config-if)#**frame-relay intf-type dce**

Cloud(config-if)#**frame-relay route *101* interface *Serial1 50***

Cloud(config-if)#**frame-relay route *102* interface *Serial2 50***

Cloud(config-if)#**exit**

Cloud(config)#**interface *Serial1***

Cloud(config-if)#**description *Frame-relay connection to Branch1 - DLCI 101***

Cloud(config-if)#**encapsulation frame-relay**

Cloud(config-if)#**clock rate *125000***

Cloud(config-if)#**frame-relay lmi-type *cisco***

Cloud(config-if)#**frame-relay intf-type dce**

Cloud(config-if)#**frame-relay route *50* interface *Serial0 101***

Cloud(config-if)#**exit**

Cloud(config)#**interface *Serial2***

Cloud(config-if)#**description *Frame-relay connection to Branch2 - DLCI 102***

Cloud(config-if)#**encapsulation frame-relay**

Cloud(config-if)#**clock rate *125000***

Cloud(config-if)#**frame-relay lmi-type *cisco***

Cloud(config-if)#**frame-relay intf-type dce**

Cloud(config-if)#**frame-relay route *50* interface *Serial0 102***

Cloud(config-if)#**exit**

Cloud(config)#**end**

Cloud#

注释 此种模拟不支持 SVC，同时对于流量整形或者与 BECN 相关的特性的支持都不是很好。**show frame-relay route** 命令来查看当前的链路交换配置。

10.7. 子接口配置下的帧中继压缩

提问 在接口配置帧中继的压缩

回答

Central#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Central(config)#**interface *Serial0***

Central(config-if)#**encapsulation frame-relay**

Central(config-if)#**frame-relay ip tcp header-compression passive**

Central(config-if)#**frame-relay payload-compression frf9 stac （packet-by-packet）**

Central(config-if)#**exit**

Central(config)#**end**

Central#

注释 passive 参数的含义是只有收到了压缩的数据包才会采用压缩。压缩模式上建议使用 FRF.9 这个开放标准。使用命令 **show frame-relay ip tcp header-compression** 可以看到压缩的统计数据

10.8. MAP 命令下的帧中继压缩

提问 配置 MAP 命令下的帧中继压缩

回答

Central#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Central(config)#**interface *Serial0***

Central(config-if)#**description *Frame Relay to branches***

Central(config-if)#**ip address *192.168.1.1 255.255.255.0***

Central(config-if)#**encapsulation frame-relay**

Central(config-if)#**frame-relay map ip *192.168.1.10 101* payload-compression frf9 stac**

Central(config-if)#**exit**

Central(config)#**end**

Central#

注释 无

10.9. 帧中继承载 PPP

提问 帧中继链路配置 PPP 封装

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *Loopback1***

Router1(config-if)#**ip address *10.1.200.5 255.255.255.252***

Router1(config-if)#**exit**

Router1(config)#**interface Virtual-Template*1***

Router1(config-if)#**ip unnumbered *Loopback1***

Router1(config-if)#**encapsulation ppp**

Router1(config-if)#**exit**

Router1(config)#**interface *Serial0***

Router1(config-if)#**no ip address**

Router1(config-if)#**encapsulation frame-relay**

Router1(config-if)#**exit**

Router1(config)#**interface *Serial0.1* point-to-point**

Router1(config-subif)#**frame-relay interface-dlci *104* ppp Virtual-Template*1***

Router1(config-fr-dlci)#**exit**

Router1(config-subif)#**exit**

Router1(config)#**end**

Router1#

注释 有点鬼...

10.10. 查看帧中继状态

提问 查看帧中继状态

回答

Central#**show interfaces *Serial0***

Central#**show frame-relay pvc**

Central#**show frame-relay lmi**

注释 无

第十一章 队列和拥塞

11.1. FAST SWITCHING 和 CEF

提问 给路由器配置最有效的包交换算法

回答

Fast Switching 缺省是启用的

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**interface *FastEthernet0/0***

Router(config-if)#**ip route-cache**

Router(config-if)#**exit**

Router(config)#**end**

Router#

如果使用策略，需要下面的命令

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**interface *FastEthernet0/0***

Router(config-if)#**ip route-cache policy**

Router(config-if)#**exit**

Router(config)#**end**

Router#

CEF 缺省是没有启用的，全局和端口启用

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**ip cef**

Router(config)#**interface *FastEthernet0/0***

Router(config-if)#**ip route-cache cef**

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 除了上面的 policy 参数以外，还有下面的参数来保证进出是同一物理接口

Router(config)#**interface *Serial0/0***

Router(config-if)#**ip route-cache same-interface**

可以使用下面命令进行验证 *show cef interface show cef drop* 和 *show cef not-cef-switched show ip cef*

11.2. 设置 DSCP 或者 TOS 位

提问 路由器标记特定数据包的 DSCP 或者 TOS 位

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**access-list *101* permit any eq *ftp* any**

Router(config)#**access-list *101* permit any any eq *ftp***

Router(config)#**access-list *102* permit any eq *ftp-data* any**

Router(config)#**access-list *102* permit any any eq *ftp-data***

Router(config)#**class-map *match-all ser00-ftpcontrol***

Router(config-cmap)#**description *branch ftp control traffic***

Router(config-cmap)#**match input-interface serial*0/0***

Router(config-cmap)#**match access-group 101**

Router(config-cmap)#**exit**

Router(config)#**class-map *match-all ser00-ftpdata***

Router(config-cmap)#**description *branch ftp data traffic***

Router(config-cmap)#**match input-interface serial*0/0***

Router(config-cmap)#**match access-group 102**

Router(config-cmap)#**exit**

Router(config)#**policy-map *serialftppolicy***

Router(config-pmap)#**description *branch ftp traffic policy***

Router(config-pmap)#**class *ser00-ftpcontrol***

Router(config-pmap-c)#**set ip precedence *immediate***

Router(config-pmap-c)#**exit**

Router(config-pmap)#**class *ser00-ftpdata***

Router(config-pmap-c)#**set ip precedence *priority***

Router(config-pmap-c)#**exit**

Router(config-pmap)#**exit**

Router(config)#**interface serial*0/0***

Router(config-if)#**ip route-cache policy**

Router(config-if)#**service-policy input *serialftppolicy***

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 先使用 classmap 来定义特殊的数据流，然后使用 policymap 来对 TOS 位进行标记

11.3. 使用优先级队列(PRIORITY QUEUING)

提问 使用优先级队列这种严格的方式来保证高优先级的数据先被处理

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**access-list *101* permit ip any any precedence *5* tos *12***

Router(config)#**access-list *102* permit ip any any precedence *4***

Router(config)#**access-list *103* permit ip any any precedence *3***

Router(config)#**priority-list *1* protocol ip high list *101***

Router(config)#**priority-list *1* protocol ip medium list *102***

Router(config)#**priority-list *1* protocol ip normal list *103***

Router(config)#**priority-list *1* default low**

Router(config)#**interface *Ethernet0***

Router(config-if)#**priority-group *1***

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 单纯使用优先级队列可能会导致高优先级的数据占用掉所有的带宽。**precedence *5* tos *12*** 等同于 **dscp ef**。缺省情况下会把不匹配的数据包归入到 normal 优先级队列，本例中特别配置其归入了 low 优先级队列。Show interface 命令可以看到缺省各个队列大小（high 优先级为 20 个，medium 为 40 个，依次递增）

Output queue (queue priority: size/max/drops):

    high: 0/20/0, medium: 0/40/0, normal 0/60/0, low 0/80/0

可以使用 Router(config)#**priority-list *1* queue-limit *10 15 25 35*** 命令来修改。建议使用 LLQ 或者 CBWFQ 来替代单纯的优先级队列

11.4. 使用自定义队列（CUSTOM QUEUING）

提问 根据数据流中 IP 优先级的不同来自定义队列共享带宽

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**access-list *103* permit ip any any precedence *5***

Router(config)#**access-list *104* permit ip any any precedence *4***

Router(config)#**access-list *105* permit ip any any precedence *3***

Router(config)#**access-list *106* permit ip any any precedence *2***

Router(config)#**access-list *107* permit ip any any precedence *1***

Router(config)#**queue-list 1 protocol ip *3* list *103***

Router(config)#**queue-list 1 protocol ip *4* list *104***

Router(config)#**queue-list 1 protocol ip *5* list *105***

Router(config)#**queue-list 1 queue 5 byte-count 3000 limit 55**

Router(config)#**queue-list 1 protocol ip *6* list *106***

Router(config)#**queue-list 1 protocol ip *7* list *107***

Router(config)#**queue-list 1 default 8**

Router(config)#**interface *HSSI0/0***

Router(config-if)#**custom-queue-list *1***

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 通过配置自定义队列可以生成 16 个应用队列和 1 个系统队列。

Queuing strategy: custom-list 1

Output queues: (queue #: size/max/drops)

0: 0/20/0 1: 0/20/0 2: 0/20/0 3: 0/20/0 4: 0/20/0

5: 0/55/3 6: 5/20/0 7: 0/20/0 8: 0/20/0 9: 0/20/0

10: 0/20/0 11: 0/20/0 12: 0/20/0 13: 0/20/0 14: 0/20/0

15: 0/20/0 16: 0/20/0

缺省情况下自定义队列不会对无分类的数据流进行队列归属，所以需要配置一个缺省队列。缺省情况下每个队列会读取 1500 字节，每个队列可最多保存 20 个数据包，可以通过 **queue-list 1 queue 5 byte-count 3000 limit 55** 命令来修改。

对于这种队列方式需要注意的是队列是基于字节的不是基于数据包的，所以对于字节下的数据流会发送相对多的数据包，但是总体来说流量是平均的。此种方式也是比较老的方案，推荐使用 CBWFQ

11.5. 自定义队列混和优先级队列

提问 高优先级数据优先处理，低优先级数据共享带宽

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**access-list *101* permit ip any any precedence *7***

Router(config)#**access-list *102* permit ip any any precedence *6***

Router(config)#**access-list *103* permit ip any any precedence *5***

Router(config)#**access-list *104* permit ip any any precedence *4***

Router(config)#**access-list *105* permit ip any any precedence *3***

Router(config)#**access-list *106* permit ip any any precedence *2***

Router(config)#**access-list *107* permit ip any any precedence *1***

Router(config)#**queue-list *1* protocol ip *1* list *101***

Router(config)#**queue-list *1* protocol ip *2* list *102***

Router(config)#**queue-list *1* protocol ip *3* list *103***

Router(config)#**queue-list *1* protocol ip *4* list *104***

Router(config)#**queue-list *1* protocol ip *5* list *105***

Router(config)#**queue-list *1* protocol ip *6* list *106***

Router(config)#**queue-list *1* protocol ip *7* list *107***

Router(config)#**queue-list *1* lowest-custom *4***

Router(config)#**interface *HSSI0/0***

Router(config-if)#**custom-queue-list *1***

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 相比 11.4 多了一个 **queue-list *1* lowest-custom *4*** ，这样 123.被定义为优先级队列

11.6. 使用加权公平队列（WEIGHTED FAIR QUEUING）

提问 根据 TOS/DSCP 位来转发数据包

回答

缺省情况下 WFQ 会自动在小于 2M 速率的接口启用

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**interface Serial*0/0***

Router(config-if)#**fair-queue *64 512 10***

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 WFQ 在没有 TOS/DSCP 标记的情况下依然可以工作。命令后面的参数分为三个，第一个为丢弃阀值，某个队列如果超过 64 个数据包，以后的数据包就会被丢弃，第二个为动态队列数目，是 16 的倍数，如果端口有很多的数据流建议增加，第三个为 RSVP 预留队列，缺省为 0。

11.7. 使用基于类的加权公平队列（USING CLASS-BASED WEIGHTED FAIR QUEUING）

提问 在端口上配置基于类的加权公平队列

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**class-map *highprec***

Router(config-cmap)#**description *Highest priority Prec=5***

Router(config-cmap)#**match ip precedence *5***

Router(config-cmap)#**exit**

Router(config)#**class-map *medhiprec***

Router(config-cmap)#**description *Medium-high priority Prec=4***

Router(config-cmap)#**match ip precedence *4***

Router(config-cmap)#**exit**

Router(config)#**class-map med*loprec***

Router(config-cmap)#**description *Medium-low priority Prec=2,3***

Router(config-cmap)#**match ip precedence *2 3***

Router(config-cmap)#**exit**

Router(config)#**policy-map *cbwfqpolicy***

Router(config-pmap)#**class *highprec***

Router(config-pmap-c)#**bandwidth percent *25***

Router(config-pmap-c)#**exit**

Router(config-pmap)#**class *medhiprec***

Router(config-pmap-c)#**bandwidth percent *25***

Router(config-pmap-c)#**exit**

Router(config-pmap)#**class med*loprec***

Router(config-pmap-c)#**bandwidth percent *25***

Router(config-pmap-c)#**exit**

Router(config-pmap)#**class class-default**

Router(config-pmap-c)#**fair-queue *512***

Router(config-pmap-c)#**queue-limit *96***

Router(config-pmap-c)#**exit**

Router(config-pmap)#**exit**

Router(config)#**interface serial*0/1***

Router(config-if)#**service-policy output *cbwfqpolicy***

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 无

11.8. 使用 NBAR

提问 使用 NBAR（Network Based Application Recognition）在应用层对数据进行识别和分类

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip cef**

Router1(config)#**class-map *INTERACTIVE***

Router1(config-cmap)#**match protocol citrix**

Router1(config-cmap)#**match protocol telnet**

Router1(config-cmap)#**exit**

Router1(config)#**policy-map *QoSPolicy***

Router1(config-pmap)#**class *INTERACTIVE***

Router1(config-pmap-c)#**bandwidth percent *50***

Router1(config-pmap-c)#**set dscp ef**

Router1(config-pmap-c)#**exit**

Router1(config-pmap)#**class class-default**

Router1(config-pmap-c)#**bandwidth percent *20***

Router1(config-pmap-c)#**random-detect dscp-based**

Router1(config-pmap-c)#**exit**

Router1(config-pmap)#**exit**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-fi)#**service-policy inbound *QoSPolicy***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

思科支持在网上下载 PDLM（Packet Description Language Module）来激活 NBAR 分类

Router1#**show flash**

System flash directory:

File Length Name/status

1 23169076 c2600-ipvoice-mz.124-10.bin

2 3100 **bittorrent.pdlm**

[23172304 bytes used, 9857836 available, 33030140 total]

32768K bytes of processor board System flash (Read/Write)

Router1#Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip nbar pdlm flash://*bittorrent.pdlm***

Router1(config)#**class-map *BITTORRENT***

Router1(config-cmap)#**match protocol *bittorrent***

Router1(config-cmap)#**exit**

Router1(config)#**end**

Router1#

也可以使用 NBAR 来自动对网络协议进行分类统计

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip nbar protocol-discovery**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 NBAR 会增加 CPU 利用率。Router1#**show ip nbar protocol-discovery top-n *5*** 可以显示出 NBAR 所识别各个协议数据统计

11.9. 使用 WRED 来控制拥塞

提问 采用 WRED 来控制拥塞

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**class-map *Prec5***

Router(config-cmap)#**description *Critical***

Router(config-cmap)#**match ip precedence *5***

Router(config-cmap)#**exit**

Router(config)#**policy-map *cb_wred***

Router(config-pmap)#**class *Prec5***

Router(config-pmap-c)#**random-detect dscp-based**

Router(config-pmap-c)#**exit**

Router(config-pmap)#**class class-default**

Router(config-pmap-c)#**fair-queue *512***

Router(config-pmap-c)#**queue-limit *96***

Router(config-pmap-c)#**random-detect dscp-based**

Router(config-pmap-c)#**exit**

Router(config-pmap)#**exit**

Router(config)#**interface HSSI*0/1***

Router(config-if)#**service-policy output *cb_wred***

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 无

11.10. 使用 RSVP

提问 在网络中启用 RSVP

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**access-list *15* permit ip *192.168.1.0 0.0.0.255***

Router(config)#**interface *FastEthernet0/0***

Router(config-if)#**ip rsvp bandwidth *128 56***

Router(config-if)#**ip rsvp neighbor *15***

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 配置 RSVP 之前，接口要配置 WFQ, CBWFQ, 或者 WRED

11.11. 手动 RSVP 预留

提问 配置手动的 RSVP 预留

回答

Sender 主机（192.168.100.202）连接 R1

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip address *192.168.100.21 255.255.255.0***

Router1(config-if)#**ip rsvp bandwidth *128 56***

Router1(config-if)#**exit**

Router1(config)#**interface *Serial0/0***

Router1(config-if)#**no ip address**

Router1(config-if)#**encapsulation frame-relay**

Router1(config-if)#**fair-queue *64 256 37***

Router1(config-if)#**ip rsvp bandwidth**

Router1(config-if)#**exit**

Router1(config)#**interface *Serial0/0.1* point-to-point**

Router1(config-subif)#**ip address *192.168.55.9 255.255.255.252***

Router1(config-subif)#**frame-relay interface-dlci *904***

Router1(config-fr-dlci)#**ip rsvp bandwidth *128 56***

Router1(config-subif)#**exit**

Router1(config)#**ip rsvp sender *192.168.9.100 192.168.100.202 UDP 1300 1300 192.168.100.202 FastEthernet0/0 55 1***

Router1(config)#**end**

Router1#

Receiver 主机（192.168.9.100）连接 R4

Router4# **configure terminal**

Router4(config)#**interface *Ethernet0/0***

Router4(config-if)#**ip address *192.168.9.3 255.255.255.0***

Router4(config-if)#**ip rsvp bandwidth *128 56***

Router4(config-if)#**exit**

Router4(config)#**interface *Serial0/0***

Router4(config-if)#**no ip address**

Router4(config-if)#**encapsulation frame-relay**

Router4(config-if)#**fair-queue *64 256 37***

Router4(config-if)#**ip rsvp bandwidth**

Router4(config-if)#**exit**

Router4(config)#**interface *Serial0/0.1* point-to-point**

Router4(config-subif)#**ip address *192.168.56.5 255.255.255.252***

Router4(config-subif)#**frame-relay interface-dlci *107***

Router4(config-fr-dlci)#**ip rsvp bandwidth *128 56***

Router4(config-subif)#**exit**

Router4(config)#**ip rsvp reservation *192.168.9.100 192.168.100.202 UDP 1300 1300 192.168.9.100 Ethernet0/0 FF RATE 55 1***

Router4(config)#**end**

Router4#

注释 无

11.12. 聚合 RSVP 的预留（AGGREGATING RSVP RESERVATIONS）

提问 聚合多个 RSVP 这样核心网络不需要对每个数据流进行追踪

回答

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**interface *FastEthernet0/0***

Router2(config-if)#**ip address *192.168.101.1 255.255.255.0***

Router2(config-if)#**ip rsvp bandwidth *128 56***

Router2(config-if)#**ip rsvp data-packet classification none**

Router2(config-if)#**ip rsvp resource-provider none**

Router2(config-if)#**exit**

Router2(config)#**interface *Serial0/0.1* point-to-point**

Router2(config-subif)#**ip address *192.168.55.10 255.255.255.252***

Router2(config-subif)#**frame-relay interface-dlci *409***

Router2(config-fr-dlci)#**ip rsvp bandwidth *128 56***

Router2(config-subif)#**ip rsvp data-packet classification none**

Router2(config-subif)#**ip rsvp resource-provider none**

Router2(config-subif)#**exit**

Router2(config)#**end**

Router2#

注释 RSVP 扩展性不强，对于核心网络还是使用传统的 DSCP 标记方式，12.2(2)T 的 IOS 引入了新的办法来解决此问题，核心路由器配置 RSVP 来支持 RSVP Requests，但是队列的时候不需要使用 RSVP 的信息

11.13. 配置一般流量整形（GENERIC TRAFFIC SHAPING）

提问 简单的方法来限制接口流量

回答

一般的限制出口流量

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**interface *FastEthernet0/0***

Router(config-if)#**traffic-shape rate *500000***

Router(config-if)#**exit**

Router(config)#**end**

Router#

和控制列表搭配使用:

```
Router#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router(config)#access-list 101 permit tcp any eq www any
Router(config)#access-list 101 permit tcp any any eq www
Router(config)#access-list 102 permit tcp any eq ftp any
Router(config)#access-list 102 permit tcp any any eq ftp
Router(config)#interface FastEthernet0/0
Router(config-if)#traffic-shape group 101 100000
Router(config-if)#traffic-shape group 102 200000
Router(config-if)#exit
Router(config)#end
Router#
```

注释 这种比较简单的控制方法只适合于不支持 CBWFQ 这种粒度更好的方式时才使用

11.14. 配置帧中继流量整形

提问 控制各个 PVC 的流量

回答

```
Router#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router(config)#interface HSSI0/0
Router(config-if)#encapsulation frame-relay
```

Router(config-if)#**exit**

Router(config)#**interface *HSSI0/0.1* point-to-point**

Router(config-subif)#**traffic-shape adaptive 10000**

Router(config-subif)#**frame-relay interface-dlci *31***

Router(config-subif)#**exit**

Router(config)#**end**

Router#

注释 *traffic-shape adaptive* 命令根据 BECN 来调整 PVC 的发送速率

11.15. 配置承诺接入速率

提问 通过配置承诺接入速率（Committed Access Rate）来控制接口的流量

回答

简单的配置平均速率为 500,000 bps，允许突发为 4500 bytes，突发超过 9000 bytes,路由器会丢弃超过的数据包:

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**interface *HSSI0/0***

Router(config-if)#**rate-limit output *500000 4500 9000* conform-action transmit exceed-action drop**

Router(config-if)#**exit**

Router(config)#**end**

Router#

使用 ACL 来定义不同的流量分类，然后限制定义不同的限制速率

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**access-list *101* permit tcp any eq *www* any**

Router(config)#**access-list *101* permit tcp any any eq *www***

Router(config)#**access-list *102* permit tcp any eq *ftp* any**

Router(config)#**access-list *102* permit tcp any any eq *ftp***

Router(config)#**access-list *102* permit tcp any eq *ftp-data* any**

Router(config)#**access-list *102* permit tcp any any eq *ftp-data***

Router(config)#**access-list *103* permit ip any any**

Router(config)#**interface *HSSI0/0***

Router(config-if)#**rate-limit output access-group *101 50000 4500 9000* conform-action transmit exceed-action drop**

Router(config-if)#**rate-limit output access-group *102 50000 4500 9000* conform-action transmit exceed-action drop**

Router(config-if)#**rate-limit output access-group *103 400000 4500 9000* conform-action transmit exceed-action drop**

Router(config-if)#**exit**

Router(config)#**end**

Router#

根据 DSCP 来控制，命令中的 DSCP 数值为十进制

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**interface *HSSI0/0***

Router(config-if)#**rate-limit output dscp *14 50000 4500 9000* conform-action transmit exceed-action drop**

Router(config-if)#**rate-limit output dscp *22 50000 4500 9000* conform-action transmit exceed-action drop**

Router(config-if)#**rate-limit output dscp *30 50000 4500 9000* conform-action transmit exceed-action drop**

Router(config-if)#**exit**

Router(config)#**end**

Router#

使用新的 rate-limiting access-list 命令格式:

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**access-list rate-limit *55 5***

Router(config)#**interface *HSSI0/0***

Router(config-if)#**rate-limit output access-group rate-limit *55 50000 4500 9000* conform-action transmit exceed-action drop**

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 在接口遇到突发数据的时候，流量整形的操作是缓存突发的包，而 CAR 是根据命令中 **exceed-action** 所定义的行为进行操作

11.16. 部署基于标准的 PHB（PER-HOP BEHAVIOR）

提问 配置基于规范的根据 DSCP 位的 PHB

回答

```
Router#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router(config)#class-map EF
Router(config-cmap)#description Real-time application traffic
Router(config-cmap)#match ip precedence 5
Router(config-cmap)#exit
Router(config)#class-map AF1x
Router(config-cmap)#description Priority Class 1
Router(config-cmap)#match ip precedence 1
Router(config-cmap)#exit
Router(config)#class-map AF2x
Router(config-cmap)#description Priority Class 2
Router(config-cmap)#match ip precedence 2
Router(config-cmap)#exit
Router(config)#class-map AF3x
Router(config-cmap)#description Priority Class 3
Router(config-cmap)#match ip precedence 3
Router(config-cmap)#exit
Router(config)#class-map AF4x
Router(config-cmap)#description Priority Class 4
Router(config-cmap)#match ip precedence 4
```

```
Router(config-cmap)#exit
Router(config)#policy-map cbwfq_pq
Router(config-pmap)#class EF
Router(config-pmap-c)#priority 58 800
Router(config-pmap-c)#exit
Router(config-pmap)#class AF1x
Router(config-pmap-c)#bandwidth percent 15
Router(config-pmap-c)#random-detect dscp-based
Router(config-pmap-c)#exit
Router(config-pmap)#class AF2x
Router(config-pmap-c)#bandwidth percent 15
Router(config-pmap-c)#random-detect dscp-based
Router(config-pmap-c)#exit
Router(config-pmap)#class AF3x
Router(config-pmap-c)#bandwidth percent 15
Router(config-pmap-c)#random-detect dscp-based
Router(config-pmap-c)#exit
Router(config-pmap)#class AF4x
Router(config-pmap-c)#bandwidth percent 15
Router(config-pmap-c)#random-detect dscp-based
Router(config-pmap-c)#exit
Router(config-pmap)#class class-default
```

Router(config-pmap-c)#**fair-queue *512***

Router(config-pmap-c)#**queue-limit *96***

Router(config-pmap-c)#**exit**

Router(config-pmap)#**exit**

Router(config)#**interface HSSI*0/1***

Router(config-if)#**service-policy output *cbwfqpolicy***

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 无

11.17. AUTOQOS

提问 配置路由器自动生成 Voip 或者一般数据包的 QoS 策略配置

回答

一种是针对 VoIP 数据的

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip cef**

Router1(config)#**interface *Serial0/0***

Router1(config-if)#**no ip address**

Router1(config-if)#**encapsulation frame-relay**

Router1(config-if)#**exit**

Router1(config)#**interface *Serial0/0.1* point-to-point**

Router1(config-subif)#**ip address *192.168.55.9 255.255.255.252***

Router1(config-subif)#**frame-relay interface-dlci *904***

Router1(config-fr-dlci)#**auto qos voip**

%Creating new map-class.

Router1(config-fr-dlci)#**exit**

Router1(config-subif)#**exit**

Router1(config)#**end**

Router1#

*Mar 1 01:32:55.031: %RMON-5-FALLINGTRAP: Falling trap is generated because the

value of cbQosCMDropBitRate.1169.1171 has fallen below the falling-threshold va

lue 0

Router1#

针对一般的 IP 数据包，第一步是流量模式的收集

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip cef**

Router1(config)#**interface *Serial0/0***

Router1(config-if)#**no ip address**

Router1(config-if)#**encapsulation frame-relay**

Router1(config-if)#**exit**

Router1(config)#**interface *Serial0/0.1* point-to-point**

Router1(config-subif)#**ip address *192.168.55.9 255.255.255.252***

Router1(config-subif)#**frame-relay interface-dlci *904***

Router1(config-fr-dlci)#**auto discovery qos**

Router1(config-fr-dlci)#**exit**

Router1(config-subif)#**exit**

Router1(config)#**end**

Router1#

第二步是生成策略

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface *Serial0/0.1* point-to-point**

Router1(config-subif)#**frame-relay interface-dlci *904***

Router1(config-fr-dlci)#**auto qos**

%Creating new map-class.

Router1(config-fr-dlci)#**no auto discovery qos**

Router1(config-fr-dlci)#**exit**

Router1(config-subif)#**exit**

Router1(config)#**end**

Router1#

注释 AutoQoS 很好，但是有下面几个限制：只能针对点对点的链路，不能和 frame map 或者 virtual templates 一起使用，不能用于 SVC，两端必须同时配置，必须禁止掉所有的服务策略或者 access-groups 即使用于其他的端口，要启用 CEF。针对 VoIP 的 AutoQoS 引自 12.2(15)T，通过一个宏来生成配置，可以用 show auto qos 来查看。针对通用 IP 数据流的引自 12.3(7)T，自动针对数据流分

类至十个不同类别，要先用 auto qos 然后再 no 掉原来的 discovery。注意的是你如果后来想不用 auto qos 了，虽然可以 no auot qos 但是还是有很多配置是没法自动清除的，记的要保存之前的 show auto qos 的输出。AutoQoS 不是万能的，要慎用

11.18. 查看队列参数

提问 查看当前端口的队列配置

回答

Router#**show queue *FastEthernet0/0***

Router#**show queuing**

注释 配置优先级队列或者自定义队列的时候 show queue 命令没有相应的输出

第十二章 隧道和 VPN

12.1. 创建 TUNNEL

提问 通过隧道的方式在网络中传输 IP 数据

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface Tunnel*1***

Router1(config-if)#**ip address *192.168.35.6 255.255.255.252***

Router1(config-if)#**tunnel source *172.25.1.5***

Router1(config-if)#**tunnel destination *172.25.1.7***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

Router5#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router5(config)#**interface Tunnel*3***

Router5(config-if)#**ip address *192.168.35.5 255.255.255.252***

Router5(config-if)#**tunnel source *172.25.1.7***

Router5(config-if)#**tunnel destination *172.25.1.5***

Router5(config-if)#**exit**

Router5(config)#**end**

Router5#

注释 Tunnel 的配置中也可以使用 **tunnel source *Ethernet0*** 的方式来捆绑到端口。产生出来的虚拟隧道接口通常会一直 UP，即使对端关机，12.2(8)T 后引入了 keeplive 参数可以对隧道的状态进行监控，**keepalive 3 2** 每隔 3 秒一个 Keeplive，如果两次没收到就认为端口当掉。如果对数据包的完整性或者防止乱序包，可以配置 **tunnel checksum**，**tunnel sequence-datagrams**，但需要注意的是 GRE 不是 TCP，数据包丢弃了不会重传。缺省情况下隧道的模式 GRE，也可以通过 **tunnel mode ipip** 命令来改变其模式。由于 GRE 是封装 IP 数据包所以不可避免地产生了 MTU 的问题，对于 TCP 连接可以使用 *ip tcp path-mtu-discovery*，但对于非 TCP 的 GRE，需要使用 **tunnel path-mtu-discovery**。在 12.2(13)T 以后引入了 **tunnel path-mtu-discovery min-mtu *500*** 来定义最小的 MTU 从而保证安全

12.2. 其他协议隧道至 IP

提问 通过隧道的方式在 IP 网络中传输其他协议数据，比如 IPX

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ipx routing *AAAA.BBBB.0001***

Router1(config)#**interface Tunnel*1***

Router1(config-if)#**ipx network *AAA***

Router1(config-if)#**tunnel source *172.25.1.5***

Router1(config-if)#**tunnel destination *172.25.1.7***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

Router5#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**ipx routing *AAAA.BBBB.0002***

Router5(config)#**interface Tunnel*3***

Router5(config-if)#**ipx network *AAA***

Router5(config-if)#**tunnel source *172.25.1.7***

Router5(config-if)#**tunnel destination *172.25.1.5***

Router5(config-if)#**exit**

Router5(config)#**end**

Router5#

注释 注意的是隧道模式里面只有 GRE 模式是支持 IPX 的。同时可以在隧道接口下配置多个不同的协议从而支持在隧道中封装多个协议

Router1(config)#**interface Tunnel*1***

Router1(config-if)#**ip address *192.168.35.6 255.255.255.252***

Router1(config-if)#**ipx network *AAA***

Router1(config-if)#**tunnel source *172.25.1.5***

Router1(config-if)#**tunnel destination *172.25.1.7***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

12.3. 隧道和动态路由协议

提问 在隧道中传递路由协议

回答

怎么解决到 tunnel destination 的路由不是通过 tunnel 接口的问题，第一种方法是静态路由

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface Tunnel*1***

Router1(config-if)#**ip address *192.168.35.6 255.255.255.252***

Router1(config-if)#**tunnel source *172.25.1.5***

Router1(config-if)#**tunnel destination *172.22.1.2***

Router1(config-if)#**exit**

Router1(config)#**ip route *172.22.1.2 255.255.255.255 172.25.1.1***

Router1(config)#**router eigrp *55***

Router1(config-router)#**network *192.168.35.0***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

第二种对 tunnel 接口采用另外的路由协议，从而排除此地址在互联的路由协议中

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface Tunnel*1***

Router1(config-if)#**ip address *192.168.35.6 255.255.255.252***

Router1(config-if)#**tunnel source *172.25.1.5***

Router1(config-if)#**tunnel destination *172.22.1.2***

Router1(config-if)#**exit**

Router1(config)#**router eigrp *55***

Router1(config-router)#**network *172.22.0.0***

Router1(config-router)#**network *172.25.0.0***

Router1(config-router)#**end**

Router1(config)#**router rip**

Router1(config-router)#**network *192.168.35.0***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

第三种方法路由过滤

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface Tunnel*1***

Router1(config-if)#**ip address *192.168.35.6 255.255.255.252***

Router1(config-if)#**tunnel source *172.25.1.5***

Router1(config-if)#**tunnel destination *172.22.1.2***

Router1(config-if)#**exit**

Router11(config)#**ip prefix-list *TUNNELROUTES* seq 10 permit *192.168.0.0/16 ge 17***

Router1(config)#**router eigrp *55***

Router1(config-router)#**network *172.22.0.0***

Router1(config-router)#**network *172.25.0.0***

Router1(config-router)#**network *192.168.35.0***

Router1(config-router)#**distribute-list prefix *TUNNELROUTES* out *Tunnel1***

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

注释 前两种很简单但是冗余性和扩展性不好，推荐第三种

12.4. 查看隧道状态

提问 查看隧道状态

回答

Router1#**show interface *Tunnel5***

Router1#**ping *192.168.66.6***

Router1#**ping *172.22.1.4***

注释 无

12.5. 在 GRE 隧道中创建一个加密的路由器到路由器的 VPN

提问 通过预共享密匙的方法创建互联网连接路由器的加密 VPN

回答

```
Router1#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router1(config)#crypto isakmp policy 10
Router1(config-isakmp)#encr aes 256
Router1(config-isakmp)#authentication pre-share
Router1(config-isakmp)#group 2
Router1(config-isakmp)#exit
Router1(config)#crypto isakmp key TUNNELKEY01 address 172.16.2.1 no-xauth
Router1(config)#crypto ipsec transform-set TUNNEL-TRANSFORM ah-sha-hmac esp-aes 256
Router1(cfg-crypto-trans)#mode transport
Router1(cfg-crypto-trans)#exit
Router1(config)#crypto map TUNNELMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router1(config-crypto-map)#set peer 172.16.2.1
Router1(config-crypto-map)#set transform-set TUNNEL-TRANSFORM
Router1(config-crypto-map)#match address 102
Router1(config-crypto-map)#exit
Router1(config)#access-list 102 permit gre host 172.16.1.1 host 172.16.2.1
Router1(config)#interface Tunnel1
```

Router1(config-if)#**ip address** ***192.168.1.1 255.255.255.252***

Router1(config-if)#**tunnel source** ***172.16.1.1***

Router1(config-if)#**tunnel destination** ***172.16.2.1***

Router1(config-if)#**exit**

Router1(config)#**interface** ***FastEthernet0/0***

Router1(config-if)#**ip address** ***172.16.1.1 255.255.255.0***

Router1(config-if)#**ip access-group** ***101*** **in**

Router1(config-if)#**crypto map** ***TUNNELMAP***

Router1(config-if)#**exit**

Router1(config)#**access-list** ***101*** **permit gre host** ***172.16.2.1*** **host** ***172.16.1.1***

Router1(config)#**access-list** ***101*** **permit esp host** ***172.16.2.1*** **host** ***172.16.1.1***

Router1(config)#**access-list** ***101*** **permit udp host** ***172.16.2.1*** **host** ***172.16.1.1*** **eq isakmp**

Router1(config)#**access-list** ***101*** **permit ahp host** ***172.16.2.1*** **host** ***172.16.1.1***

Router1(config)#**access-list** ***101*** **deny ip any any log**

Router1(config)#**interface** ***Loopback0***

Router1(config-if)#**ip address** ***192.168.16.1 255.255.255.0***

Router1(config-if)#**exit**

Router1(config)#**ip route 0.0.0.0 0.0.0.0** ***172.16.1.2***

Router1(config)#**ip route** ***192.168.15.0 255.255.255.0 192.168.1.2***

Router1(config)#**end**

Router1#

Router2#**configure terminal**

```
Enter configuration commands, one per line.    End with CNTL/Z.
Router2(config)#crypto isakmp policy 10
Router2(config-isakmp)#encr aes 256
Router2(config-isakmp)#authentication pre-share
Router2(config-isakmp)#group 2
Router2(config-isakmp)#exit
Router2(config)#crypto isakmp key TUNNELKEY01 address 172.16.1.1
Router2(config)#crypto ipsec transform-set TUNNEL-TRANSFORM ah-sha-hmac esp-aes 256
Router2(cfg-crypto-trans)#mode transport
Router2(cfg-crypto-trans)#exit
Router2(config)#crypto map TUNNELMAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router2(config-crypto-map)#set peer 172.16.1.1
Router2(config-crypto-map)#set transform-set TUNNEL-TRANSFORM
Router2(config-crypto-map)#match address 102
Router2(config-crypto-map)#exit
Router2(config)#access-list 102 permit gre host 172.16.2.1 host 172.16.1.1
Router2(config)#interface Tunnel1
Router2(config-if)#ip address 192.168.1.2 255.255.255.252
Router2(config-if)#tunnel source 172.16.2.1
Router2(config-if)#tunnel destination 172.16.1.1
```

Router2(config-if)#**exit**

Router2(config)#**interface** ***FastEthernet0/0***

Router2(config-if)#**ip address** ***172.16.2.1 255.255.255.0***

Router2(config-if)#**ip access-group** ***101*** **in**

Router2(config-if)#**crypto map** ***TUNNELMAP***

Router2(config-if)#**exit**

Router2(config)#**access-list** ***101*** **permit gre host** ***172.16.1.1*** **host** ***172.16.2.1***

Router2(config)#**access-list** ***101*** **permit esp host** ***172.16.1.1*** **host** ***172.16.2.1***

Router2(config)#**access-list** ***101*** **permit udp host** ***172.16.1.1*** **host** ***172.16.2.1*** **eq isakmp**

Router2(config)#**access-list** ***101*** **permit ahp host** ***172.16.1.1*** **host** ***172.16.2.1***

Router2(config)#**access-list** ***101*** **deny ip any any log**

Router2(config)#**interface** ***Loopback0***

Router2(config-if)#**ip address** ***192.168.15.1 255.255.255.0***

Router2(config-if)#**exit**

Router2(config)#**ip route 0.0.0.0 0.0.0.0** ***172.16.2.2***

Router2(config)#**ip route** ***192.168.16.0 255.255.255.0 192.168.1.1***

Router2(config)#**end**

Router2#

注释 第一步首先使用 ISAKMP 来生成合适的密匙交换策略，当双方协商 SA 参数时，先从优先级低的策略开始，使用 show crypto isakmp policy 来查看当前策略。然后定义初始的密匙 crypto isakmp key,这里可以基于 IP 地址也可以基于主机名，如果基于主机名对端要配置 **crypto isakmp identity hostname**，用 show crypto isakmp key 来验证。**show crypto isakmp sa** 用来查看协商的 ISAKMP SA 状态，而最后的 IPSec SA 通过 **show crypto ipsec sa** 来查看。下一步是定义 IPSec 的 transform set，是定义如何处理符合的数据包，并且要定义 Ipsec 的透明模式，缺省使用隧道模式，对于 GRE 使用透明

模式，GRE 隧道比传统的 IPSec 隧道好在更简单和更灵活，比如可以传递动态路由协议等。最后使用 crypto map 命令整合。最后要注意的是 crypto map 应用于接收 GRE 数据包的接口而不是 tunnel 接口。**show crypto engine connections active** 显示当前连接情况

12.6. 在两个路由器的 LAN 接口之间创建加密 VPN

提问 使用预共享密匙的方式创建加密 VPN 通过互联网连接的两个 LAN 接口

回答

R1

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**crypto isakmp policy *10***

Router1(config-isakmp)#**encr aes *256***

Router1(config-isakmp)#**authentication pre-share**

Router1(config-isakmp)#**group *2***

Router1(config-isakmp)#**exit**

Router1(config)#**crypto isakmp key *TUNNELKEY01* address *172.16.2.1* no-xauth**

Router1(config)#**crypto ipsec transform-set *LAN2LAN-TRANSFORM* ah-sha-hmac esp-aes *256***

Router1(cfg-crypto-trans)#**exit**

Router1(config)#**access-list *102* permit gre host *172.16.1.1* host *172.16.2.1***

Router1(config)#**crypto map LAN2LANMAP *10* ipsec-isakmp**

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

Router1(config-crypto-map)#**set peer *172.16.2.1***

Router1(config-crypto-map)#**set transform-set *LAN2LAN-TRANSFORM***

Router1(config-crypto-map)#**match address *103***

Router1(config-crypto-map)#**exit**

Router1(config)#**access-list *103* permit ip *192.168.16.0 0.0.0.255 192.168.15.0 0.0.0.255***

Router1(config)#**interface *FastEthernet0/1***

Router1(config-if)#**ip address *192.168.16.1 255.255.255.0***

Router1(config-if)#**exit**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip address *172.16.1.1 255.255.255.0***

Router1(config-if)#**ip access-group *101* in**

Router1(config-if)#**crypto map *LAN2LANMAP***

Router1(config-if)#**exit**

Router1(config)#**ip route *0.0.0.0 0.0.0.0 172.16.1.2***

Router1(config)#**access-list *101* permit esp host *172.16.2.1* host *172.16.1.1***

Router1(config)#**access-list *101* permit udp host *172.16.2.1* host *172.16.1.1* eq isakmp**

Router1(config)#**access-list *101* permit ahp host *172.16.2.1* host *172.16.1.1***

Router1(config)#**access-list *101* deny ip any any log**

Router1(config)#**end**

Router1#

R2

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**crypto isakmp policy *10***

Router2(config-isakmp)#**encr aes *256***

Router2(config-isakmp)#**authentication pre-share**

Router2(config-isakmp)#**group *2***

Router2(config-isakmp)#**exit**

Router2(config)#**crypto isakmp key *TUNNELKEY01* address *172.16.1.1***

Router2(config)#**crypto ipsec transform-set *LAN2LAN-TRANSFORM* ah-sha-hmac esp-aes *256***

Router2(cfg-crypto-trans)#**exit**

Router2(config)#**crypto map *LAN2LANMAP 10* ipsec-isakmp**

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

Router2(config-crypto-map)#**set peer *172.16.1.1***

Router2(config-crypto-map)#**set transform-set *LAN2LAN-TRANSFORM***

Router2(config-crypto-map)#**match address *103***

Router2(config-crypto-map)#**exit**

Router2(config)#**access-list *103* permit ip *192.168.15.0 0.0.0.255 192.168.16.0 0.0.0.255***

Router2(config)#**interface *FastEthernet0/1***

Router2(config-if)#**description *Internal LAN***

Router2(config-if)#**ip address *192.168.15.1 255.255.255.0***

Router2(config-if)#**exit**

Router2(config)#**interface *FastEthernet0/0***

Router2(config-if)#**description *Connection to Internet***

Router2(config-if)#**ip address *172.16.2.1 255.255.255.0***

Router2(config-if)#**crypto map *LAN2LANMAP***

Router2(config-if)#**exit**

Router2(config)#**ip route *0.0.0.0 0.0.0.0 172.16.2.2***

Router2(config)#**access-list *101* permit esp host *172.16.1.1* host *172.16.2.1***

Router2(config)#**access-list *101* permit udp host *172.16.1.1* host *172.16.2.1* eq isakmp**

Router2(config)#**access-list *101* permit ahp host *172.16.1.1* host *172.16.2.1***

Router2(config)#**access-list *101* deny ip any any log**

Router2(config)#**end**

Router2#

注释 这里跟前节区别在于 12.5 建立的是可路由的加密 VPN。前面配置了 **mode transport** 而这里使用了 IPSec 隧道缺省的隧道模式。在 ACL 配置上前者允许的是 GRE 的数据包，这里是内部 LAN 接口之间的数据包，所以这里两个互联是桥接，前者两个互联是路由。通常我们更喜欢路由模式多一些

12.7. 生成 RSA 密匙

提问 生成共享的 RSA 密匙用于加密或者认证

回答

先在 R1 上生成自己的 pubkey

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**crypto key generate rsa**

The name for the keys will be: Router1.oreilly.com

```
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
Generating RSA keys ...
[OK]

Router1(config)#end
Router1#show crypto key mypubkey rsa
% Key pair was generated at: 01:19:45 EST Mar 1 2003
Key name: Router1.oreilly.com
 Usage: General Purpose Key
 Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E68338
  D561B2D1 7B8B75D6 7B34F6AF 1710B00B 5B6E9E8D D7183BE6 F08A6342 054EADFC
  B764DF9C 4592B891 522727F2 14233B47 8F757134 24F03DB3 833C5988 312B11E9
  FB6E0E20 4579C0A4 F2062353 4F1C8CE4 410EE57B 9FCEE784 DA7E3852 408E9742
  2584DF56 67293F3F F76B6A96 C4D518FB 1A0114BF E2449838 BE5794E2 37020301 0001
% Key pair was generated at: 01:19:52 EST Mar 1 2003
Key name: Router1.oreilly.com.server
 Usage: Encryption Key
```

Key Data:

307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00BD928A BD5637E6

2265621C 3AC57138 911CA27D 11F40AA1 E657EA26 6EBF654C 952A3319 D421A33C

E2ECA87E CD7E050C 8A8FE64D B73954EA BF2ED639 BC6A8F74 5B9550EA 4119E796

A97430E2 4B1BF7D3 ED1469FF AEA83690 A0FEA871 BBFBE8AD 19020301 0001

Router1#

然后拷贝粘贴到对端路由器

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**crypto key pubkey-chain rsa**

Router2(config-pubkey-chain)#**addressed-key *192.168.99.1***

Router2(config-pubkey-key)#**address *192.168.99.1***

Router2(config-pubkey-key)#**key-string**

Enter a public key as a hexidecimal number ....

Router2(config-pubkey)#***30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E68338***

Router2(config-pubkey)#***D561B2D1 7B8B75D6 7B34F6AF 1710B00B 5B6E9E8D D7183BE6 F08A6342 054EADFC***

Router2(config-pubkey)#***B764DF9C 4592B891 522727F2 14233B47 8F757134 24F03DB3 833C5988 312B11E9***

Router2(config-pubkey)#***FB6E0E20 4579C0A4 F2062353 4F1C8CE4 410EE57B 9FCEE784 DA7E3852 408E9742***

Router2(config-pubkey)#***2584DF56 67293F3F F76B6A96 C4D518FB 1A0114BF E2449838 BE5794E2 37020301 0001***

Router2(config-pubkey)#**quit**

Router2(config-pubkey-key)#**exit**

Router2(config-pubkey-chain)#**exit**

Router2(config)#**end**

Router2#**show crypto key pubkey-chain rsa address *192.168.99.1***

Key address: 192.168.99.1

Usage: General Purpose Key

Source: Manually entered

Data:

30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00E68338

D561B2D1 7B8B75D6 7B34F6AF 1710B00B 5B6E9E8D D7183BE6 F08A6342 054EADFC

B764DF9C 4592B891 522727F2 14233B47 8F757134 24F03DB3 833C5988 312B11E9

FB6E0E20 4579C0A4 F2062353 4F1C8CE4 410EE57B 9FCEE784 DA7E3852 408E9742

2584DF56 67293F3F F76B6A96 C4D518FB 1A0114BF E2449838 BE5794E2 37020301 0001

Router2#

注释 由于密匙里面包含路由器名和域名，所以必须首先配置

Router1(config)#**hostname *Router1***

Router1(config)#**ip domain-name *oreilly.com***

如果修改上面配置则密匙无效。通过命令 **crypto key zeroize rsa** 来删除当前密匙

12.8. 使用 RSA 密匙创建路由器到路由器的 VPN

提问 利用 RSA 密匙创建一个加密的 VPN

回答

R1

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**crypto key pubkey-chain rsa**

Router1(config-pubkey-chain)#**addressed-key *172.16.2.1***

Router1(config-pubkey-key)#**address *172.16.2.1***

Router1(config-pubkey-key)#**key-string**

Enter a public key as a hexidecimal number ....

Router1(config-pubkey)#***30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00EB0AB2***

Router1(config-pubkey)#***EA33B519 0CD95EFF EDFD4723 BED73640 97981CC0 1FC83FBF 5C6DF97C 8CB8CE0A***

Router1(config-pubkey)#***C5FE959D 1E055002 83B92EF4 35B69545 C3217E5F E0C32A73 44FD2373 15979E77***

Router1(config-pubkey)#***75598BE0 B4A4E7B2 3C318C2D 3BF3B192 8B71D8C9 A1E0F929 0E84BDAD EC909833***

Router1(config-pubkey)#***BC425170 400BD26A 319E632F 4E9649F5 BA7ADA40 5A94B09C 05F8414E 33020301 0001***

Router1(config-pubkey)#**quit**

Router1(config-pubkey-key)#**exit**

Router1(config-pubkey-chain)#**exit**

Router1(config)#**crypto isakmp policy** 100

Router1(config-isakmp)#**encryption aes** 256

Router1(config-isakmp)#**authentication rsa-encr**

Router1(config-isakmp)#**group** 2

Router1(config-isakmp)#**exit**

Router1(config)#**crypto ipsec transform-set *TUNNEL-TRANSFORM* ah-sha-hmac esp-aes *256***

Router1(cfg-crypto-trans)#**mode transport**

Router1(cfg-crypto-trans)#**exit**

Router1(config)#**crypto map *TUNNEL-RSA 10* ipsec-isakmp**

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

Router1(config-crypto-map)#**set peer *172.16.2.1***

Router1(config-crypto-map)#**set transform-set *TUNNEL-TRANSFORM***

Router1(config-crypto-map)#**match address *102***

Router1(config-crypto-map)#**exit**

Router1(config)#**access-list *102* permit gre host *172.16.1.1* host *172.16.2.1***

Router1(config)#**interface Tunnel*1***

Router1(config-if)#**ip address *192.168.1.1 255.255.255.252***

Router1(config-if)#**tunnel source *172.16.1.1***

Router1(config-if)#**tunnel destination *172.16.2.1***

Router1(config-if)#**exit**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip address *172.16.1.1 255.255.255.0***

Router1(config-if)#**ip access-group *101* in**

Router1(config-if)#**crypto map *TUNNEL-RSA***

Router1(config-if)#**exit**

Router1(config)#**access-list *101* permit gre host *172.16.2.1* host *172.16.1.1***

Router1(config)#**access-list *101* permit esp host *172.16.2.1* host *172.16.1.1***

Router1(config)#**access-list *101* permit udp host *172.16.2.1* host *172.16.1.1* eq isakmp**

Router1(config)#**access-list *101* permit ahp host *172.16.2.1* host *172.16.1.1***

Router1(config)#**access-list *101* deny ip any any log**

Router1(config)#**end**

Router1#

R2

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**crypto key pubkey-chain rsa**

Router2(config-pubkey-chain)#**addressed-key *172.16.1.1***

Router2(config-pubkey-key)#**address *172.16.1.1***

Router2(config-pubkey-key)#**key-string**

Enter a public key as a hexidecimal number ....

Router2(config-pubkey)#**30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00A0830E**

Router2(config-pubkey)#**01E4B6E1 08823E41 8A98A7F4 DB0E6277 1E7AA500 F7B620CA 49BCBEBA B0A0455A**

Router2(config-pubkey)#**114BA6B9 5ADE0D2E 7DC3EFC1 D7D07015 01C83E08 7305ED3C 71F04B44 31A1C574**

Router2(config-pubkey)#**C0E6ACA2 C191DB07 3D347F88 2D2884BF 99C2AF80 45BC1BE9 6D2BF684 B60C04E6**

Router2(config-pubkey)#**0F3D5C09 7C26694F 8FB75F90 2FA1DF46 94401D54 82ACA366 E621DD04 4B020301 0001**

Router2(config-pubkey)#**quit**

Router2(config-pubkey-key)#**exit**

Router2(config-pubkey-chain)#**exit**

Router2(config)#**crypto isakmp policy *100***

Router2(config-isakmp)#**encryption aes 256**

Router2(config-isakmp)#**authentication rsa-encr**

Router2(config-isakmp)#**group *2***

Router2(config-isakmp)#**exit**

Router2(config)#**crypto ipsec transform-set *TUNNEL-TRANSFORM* ah-sha-hmac esp-aes *256***

Router2(cfg-crypto-trans)#**mode transport**

Router2(cfg-crypto-trans)#**exit**

Router2(config)#**crypto map *TUNNEL-RSA 10* ipsec-isakmp**

Router2(config-crypto-map)#**set peer *172.16.1.1***

Router2(config-crypto-map)#**set transform-set *TUNNEL-TRANSFORM***

Router2(config-crypto-map)#**match address *102***

Router2(config-crypto-map)#**exit**

Router2(config)#**access-list *102* permit gre host *172.16.2.1* host *172.16.1.1***

Router2(config)#**interface *Tunnel1***

Router2(config-if)#**ip address *192.168.1.2 255.255.255.252***

Router2(config-if)#**tunnel source *172.16.2.1***

Router2(config-if)#**tunnel destination *172.16.1.1***

Router2(config-if)#**exit**

Router2(config)#**interface *FastEthernet0/0***

Router2(config-if)#**ip address *172.16.1.1 255.255.255.0***

Router2(config-if)#**ip access-group *101* in**

Router2(config-if)#**crypto map *TUNNEL-RSA***

Router2(config-if)#**exit**

Router2(config)#**access-list *101* permit gre host *172.16.1.1* host *172.16.2.1***

Router2(config)#**access-list *101* permit esp host *172.16.1.1* host *172.16.2.1***

Router2(config)#**access-list *101* permit udp host *172.16.1.1* host *172.16.2.1* eq isakmp**

Router2(config)#**access-list *101* permit ahp host *172.16.1.1* host *172.16.2.1***

Router2(config)#**access-list *101* deny ip any any log**

Router2(config)#**end**

Router2#

注释 类似 12.3 和 12.6

12.9. 创建主机到路由器的 VPN

提问 从远端主机到路由器的 VPN 连接

回答

只有路由器的配置，没有主机上软件的配置

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**aaa new-model**

Router1(config)#**aaa authentication login default group tacacs+**

Router1(config)#**aaa authentication enable default group tacacs+**

Router1(config)#**tacacs-server host *172.25.1.1***

Router1(config)#**tacacs-server key *NEOSHI***

Router1(config)#**crypto isakmp policy *10***

Router1(config-isakmp)#**encryption 3des**

Router1(config-isakmp)#**authentication pre-share**

Router1(config-isakmp)#**group *2***

Router1(config-isakmp)#**exit**

Router1(config)#**crypto ipsec transform-set *VPN-TRANSFORMS* ah-sha-hmac esp-sha-hmac esp-3des**

Router1(cfg-crypto-trans)#**mode tunnel**

Router1(cfg-crypto-trans)#**exit**

Router1(config)#**crypto dynamic-map *VPN-USER-MAP 50***

Router1(config-crypto-map)#**description *A dynamic crypto map for VPN users***

Router1(config-crypto-map)#**match address *115***

Router1(config-crypto-map)#**set transform-set *VPN-TRANSFORMS***

Router1(config-crypto-map)#**exit**

Router1(config)#**access-list *115* deny any *224.0.0.0 35.255.255.255***

Router1(config)#**access-list *115* deny any *172.25.1.255 0.0.0.0***

Router1(config)#**access-list *115* permit any any**

Router1(config)#**crypto map *CRYPTOMAP 10* ipsec-isakmp dynamic *VPN-USER-MAP***

Router1(config)#**interface *FastEthernet0/1***

Router1(config-if)#**ip address *172.25.1.5 255.255.255.0***

Router1(config-if)#**crypto map *CRYPTOMAP***

Router1(config-if)#**exit**

Router1(config)#**exit**

Router1#

注释 由于主机可能来自任意地址所以这里使用过了 dynamic crypto maps

12.10. 创建 SSL VPN

提问 使用路由器的 WebVPN 服务来创建 SSL VPN

回答

Core#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Core(config)#**hostname *Core***

Core(config)#**ip domain-name *oreilly.com***

Core(config)#**aaa new-model**

Core(config)#**aaa authentication login *local_auth* local**

Core(config)#**username ijbrown secret *ianspassword***

Core(config)#**username kdooley secret *kevinspassword***

Core(config)#**crypto pki trustpoint *WEBVPN***

Core(ca-trustpoint)#**enrollment selfsigned**

Core(ca-trustpoint)#**rsakeypair *WEBVPN 1024***

Core(ca-trustpoint)#**subject-name *CN=WEBVPN OU=cookbooks O=oreilly***

Core(ca-trustpoint)#**exit**

Core(config)#**crypto pki enroll *WEBVPN***

The router has already generated a Self Signed Certificate for

trustpoint TP-self-signed-3299111097.

If you continue the existing trustpoint and Self Signed Certificate

will be deleted.

Do you want to continue generating a new Self Signed Certificate? [yes/no]:**yes**

% Include the router serial number in the subject name? [yes/no]: **no**

% Include an IP address in the subject name? [no]: **no**

Generate Self Signed Router Certificate? [yes/no]: **yes**

Router Self Signed Certificate successfully created

Core(config)#**interface *Loopback0***

Core(config-if)#**ip address** ***172.25.100.2 255.255.255.255***

Core(config-if)#**exit**

Core(config)#**webvpn enable gateway-addr** ***172.25.100.2***

Core(config)# Core(config)#**webvpn**

Core(config-webvpn)#**ssl trustpoint** ***WEBVPN***

Core(config-webvpn)#**ssl encryption 3des-sha1**

Core(config-webvpn)#**title "*Cisco Cookbook WebVPN Portal*"**

Core(config-webvpn)#**url-list** ***COOKBOOKURLS***

Core(config-webvpn-url)#**heading "*Cookbook URLs*"**

Core(config-webvpn-url)#**url-text "*Cisco Cookbook*" url-value "*http://www.oreilly.com/catalog/ciscockbk/*"**

Core(config-webvpn-url)#**url-text "*Perl Cookbook*" url-value**

"*http://www.oreilly.com/catalog/perlckbk2/*"

Core(config-webvpn-url)#**heading "*Cisco URLs*"**

Core(config-webvpn-url)#**url-text "*The Books*" url-value**

"*http://www.oreilly.com/pub/topic/cisco*"

Core(config-webvpn-url)#**exit**

Core(config-webvpn)#**port-forward list** ***SERVERLOGIN*** **local-port** ***20003*** **remote-server** ***172.25.1.1*** **remote-port** ***23***

Core(config-webvpn)#**exit**

Core(config)#**end**

Core#

注释 12.3(14)T 引入了 WebVPN 服务，但是只能在特定的平台上，只能支持 SSLv3，不支持 TLS，不支持思科 SSL VPN 客户端软件。附带说一下最后的 port forward 配置，当用户连接上 WebVPN 后，使用 telnet 到本地的 20003 端口就会转发至 172.25.1.1 的 23 端口

12.11. 查看 IPSEC 协议状态

提问 查看 VPN 状态

回答

显示 ISAKMP security associations.

Router1#**show crypto isakmp sa**

IPSec security associations

Router1#**show crypto ipsec sa**

查看活动的 IPSec 连接

Router1#**show crypto engine connections active**

查看被丢弃的数据包

Router1#**show crypto engine connections dropped-packet**

查看配置的 IPSec crypto maps

Router1#**show crypto map**

对于 dynamic crypto maps

Router1#**show crypto dynamic-map**

注释 无

第十三章 拨号备份

13.1. 自动拨号备份

提问 当广域网链路中断的时候自动拨号恢复备份链路

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface *BRI0/0***

Router1(config-if)#**ip address *10.1.99.55 255.255.255.0***

Router1(config-if)#**encapsulation ppp**

Router1(config-if)#**dialer idle-timeout *300***

Router1(config-if)#**dialer map ip *10.1.99.1* name *dialhost* broadcast *95551212***

Router1(config-if)#**dialer load-threshold *50* either**

Router1(config-if)#**dialer-group *1***

Router1(config-if)#**isdn switch-type basic-ni**

Router1(config-if)#**isdn spid1 *800555123400 5551234***

Router1(config-if)#**isdn spid2 *800555123500 5551235***

Router1(config-if)#**ppp authentication chap**

Router1(config-if)#**ppp multilink**

Router1(config-if)#**exit**

Router1(config)#**username *dialhost* password *dialpassword***

Router1(config)#**ip route *0.0.0.0 0.0.0.0 10.1.99.1 180***

Router1(config)#**dialer-list *1* protocol ip list *101***

Router1(config)#**access-list *101* deny eigrp any any**

Router1(config)#**access-list *101* permit ip any any**

Router1(config)#**router eigrp *55***

Router1(config-router)#**network *10.0.0.0***

Router1(config-router)#**end**

Router1#

注释 **isdn switch-type** 定义对端ISDN交换机类型，中国用basic-net3。通过Router1#**show isdn status** 来查看当前状态

Router1#**show isdn status**

Global ISDN Switchtype = basic-ni

ISDN BRI1/0 interface

dsl 8, interface ISDN Switchtype = basic-ni

Layer 1 Status:

ACTIVE

Layer 2 Status:

TEI = 85, Ces = 1, SAPI = 0, State = **MULTIPLE_FRAME_ESTABLISHED**

TEI = 86, Ces = 2, SAPI = 0, State = **MULTIPLE_FRAME_ESTABLISHED**

TEI 85, ces = 1, state = 8(established)

spid1 configured, spid1 sent, spid1 valid

TEI 86, ces = 2, state = 8(established)

spid2 configured, spid2 sent, spid2 valid

Layer 3 Status:

0 Active Layer 3 Call(s)

Activated dsl 8 CCBs = 0

The Free Channel Mask: 0x80000003

Total Allocated ISDN CCBs = 2

Router1#

说明的是关注流量触发了拨号接通以后所有的数据都可以传输，不仅仅是关注流量

13.2. 使用拨号接口

提问 捆绑多个物理接口为一个拨号接口

回答

捆绑两个 ISDN BRI 接口

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *BRI0/0***

Router1(config-if)#**encapsulation ppp**

Router1(config-if)#**dialer pool-member *1***

Router1(config-if)#**isdn switch-type basic-ni**

Router1(config-if)#**isdn spid1 *800555123400 5551234***

Router1(config-if)#**isdn spid2 *800555123500 5551235***

Router1(config-if)#**ppp authentication chap**

Router1(config-if)#**exit**

Router1(config)#**interface *BRI0/1***

Router1(config-if)#**encapsulation ppp**

Router1(config-if)#**dialer pool-member *1***

Router1(config-if)#**isdn switch-type basic-ni**

Router1(config-if)#**isdn spid1 *800555123600 5551236***

Router1(config-if)#**isdn spid2 *800555123700 5551237***

Router1(config-if)#**ppp authentication chap**

Router1(config-if)#**exit**

Router1(config)#**interface *Dialer1***

Router1(config-if)#**ip address *10.1.99.55 255.255.255.0***

Router1(config-if)#**encapsulation ppp**

Router1(config-if)#**dialer remote-name *dialhost***

Router1(config-if)#**dialer pool *1***

Router1(config-if)#**dialer idle-timeout *300***

Router1(config-if)#**dialer string *95551212***

Router1(config-if)#**dialer load-threshold *50* either**

Router1(config-if)#**dialer-group *1***

Router1(config-if)#**ppp authentication chap**

Router1(config-if)#**ppp multilink**

Router1(config-if)#**exit**

Router1(config)#**username *dialhost* password *dialpassword***

Router1(config)#**ip route *0.0.0.0 0.0.0.0 10.1.99.1 180***

Router1(config)#**dialer-list *1* protocol ip list *101***

Router1(config)#**access-list *101* deny eigrp any any**

Router1(config)#**access-list *101* permit ip any any**

Router1(config)#**router eigrp *55***

Router1(config-router)#**network *10.0.0.0***

Router1(config-router)#**end**

Router1#

主机端

dialhost#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

dialhost(config)#**username *Router1* password *dialpassword***

dialhost(config)#**controller T1 *0***

dialhost(config-controller)#**framing esf**

dialhost(config-controller)#**clock source line primary**

dialhost(config-controller)#**linecode b8zs**

dialhost(config-controller)#**pri-group timeslots *1-24***

dialhost(config-controller)#**exit**

dialhost(config)#**interface *Serial0:23***

dialhost(config-if)#**encapsulation ppp**

dialhost(config-if)#**dialer rotary-group *1***

dialhost(config-if)#**dialer-group *1***

dialhost(config-if)#**isdn switch-type *primary-dms100***

dialhost(config-if)#**isdn not-end-to-end *56***

dialhost(config-if)#**exit**

dialhost(config)#**interface *Dialer1***

dialhost(config-if)#**ip address *10.1.99.1 255.255.255.0***

dialhost(config-if)#**encapsulation ppp**

dialhost(config-if)#**dialer in-band**

dialhost(config-if)#**dialer idle-timeout *300***

dialhost(config-if)#**dialer-group *1***

dialhost(config-if)#**no peer default ip address**

dialhost(config-if)#**ppp authentication chap**

dialhost(config-if)#**ppp multilink**

dialhost(config-if)#**exit**

dialhost(config)#**access-list *101* deny eigrp any any**

dialhost(config)#**access-list *101* permit ip any any**

dialhost(config)#**dialer-list *1* protocol ip list *101***

dialhost(config)#**router eigrp *55***

dialhost(config-router)#**network *10.0.0.0***

dialhost(config-router)#**exit**

dialhost(config)#**end**

dialhost#

注释 本节实现的结果和 13.1 相同，配置也基本相同，不同的是这里没有使用 dialer map 命令，在物理接口上也没有配置 IP 地址，相关配置都在定义的逻辑拨号接口 Dialer1 上。在 Server 端使用了 PRI

13.3. 在 AUX 端口使用异步 MODEM

提问 在路由器的 AUX 端口连接异步 Modem，用其作为拨号备份

回答

Router2#**configure terminal**

```
Enter configuration commands, one per line.    End with CNTL/Z.
Router2(config)#interface Async65
Router2(config-if)#encapsulation ppp
Router2(config-if)#dialer in-band
Router2(config-if)#dialer pool-member 1
Router2(config-if)#ppp authentication chap
Router2(config-if)#async default routing
Router2(config-if)#exit
Router2(config)#interface Dialer1
Router2(config-if)#ip address 10.1.99.56 255.255.255.0
Router2(config-if)#encapsulation ppp
Router2(config-if)#dialer remote-name dialhost
Router2(config-if)#dialer pool 1
Router2(config-if)#dialer idle-timeout 300
Router2(config-if)#dialer string 95551212
Router2(config-if)#dialer-group 1
Router2(config-if)#ppp authentication chap
Router2(config-if)#exit
Router2(config)#line aux 0
Router2(config-line)#modem inout
Router2(config-line)#transport input all
Router2(config-line)#no exec
```

Router2(config-line)#**speed *115200***

Router2(config-line)#**exit**

Router2(config)#**username *dialhost* password *dialpassword***

Router2(config)#**ip route *0.0.0.0 0.0.0.0 10.1.99.1 180***

Router2(config)#**dialer-list *1* protocol ip list *101***

Router2(config)#**access-list *101* deny eigrp any any**

Router2(config)#**access-list *101* permit ip any any**

Router2(config)#**router eigrp *55***

Router2(config-router)#**network *10.0.0.0***

Router2(config-router)#**exit**

Router2(config)#**end**

Router2#

注释 开始要先通过 show line 查找出 AUX 口的 vty 号码，也就是 **interface *Async65*** ，然后使用前面提到的拨号接口的方法进行配置，多了一个 async default routing 命令，因为缺省情况下异步口是禁止启用路由协议的。在对 AUX 端口配置时，首先一定要使用 no exec 来避免出现 Modem 不能响应的问题，同时建议调整速率，否则会缺省 9.6 Kbps。

13.4. 使用备份接口

提问 在广域网物理接口断掉的情况下拨号

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface *Serial0/0***

Router1(config-if)#**backup delay *0 300***

Router1(config-if)#**backup interface** ***BRI0/0***

Router1(config-if)#**encapsulation frame-relay**

Router1(config-if)#**down-when-looped**

Router1(config-if)#**exit**

Router1(config)#**interface** ***Serial0/0.1*** **point-to-point**

Router1(config-subif)#**ip address** ***10.1.1.10 255.255.255.252***

Router1(config-subif)#**frame-relay interface-dlci** ***50***

Router1(config-subif)#**exit**

Router1(config)#**interface** ***BRI0/0***

Router1(config-if)#**ip address** ***10.1.99.55 255.255.255.0***

Router1(config-if)#**encapsulation ppp**

Router1(config-if)#**dialer idle-timeout** ***300***

Router1(config-if)#**dialer map ip** ***10.1.99.1*** **name** ***dialhost*** **broadcast** ***95551212***

Router1(config-if)#**dialer load-threshold** ***50*** **either**

Router1(config-if)#**dialer-group** ***1***

Router1(config-if)#**isdn switch-type basic-ni**

Router1(config-if)#**isdn spid1** ***800555123400 5551234***

Router1(config-if)#**isdn spid2** ***800555123500 5551235***

Router1(config-if)#**ppp authentication chap**

Router1(config-if)#**ppp multilink**

Router1(config-if)#**exit**

Router1(config)#**dialer-list** ***1*** **protocol ip permit**

Router1(config)#**end**

Router1#

注释 备份接口的配置要放在物理接口上而不是子接口上。一般不推荐使用此方法进行备份，因为很多广域网链路的问题不能体现在物理接口 down 掉上，并且在正常情况下会使备份接口处于禁用状态，这样会需要重新拨号，不能使用 show isdn status 等命令进行查看状态等问题。

13.5. 使用 DIALER WATCH

提问 使用思科的 Dialer Watch 特性来触发拨号备份

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *BRI0/0***

Router1(config-if)#**ip address *10.1.99.55 255.255.255.0***

Router1(config-if)#**encapsulation ppp**

Router1(config-if)#**dialer map ip *10.1.1.0* name dialhost broadcast *95551212***

Router1(config-if)#**dialer map ip *10.2.0.0* name dialhost broadcast *95551212***

Router1(config-if)#**dialer map ip *10.1.99.1* name dialhost broadcast *95551212***

Router1(config-if)#**dialer load-threshold *50* either**

Router1(config-if)#**dialer watch-group *1***

Router1(config-if)#**dialer-group *1***

Router1(config-if)#**isdn switch-type basic-ni**

Router1(config-if)#**isdn spid1 *800555123400 5551234***

Router1(config-if)#**isdn spid2 *800555123500 5551235***

Router1(config-if)#**ppp authentication chap**

Router1(config-if)#**ppp multilink**

Router1(config-if)#**exit**

Router1(config)#**router eigrp *55***

Router1(config-router)#**network *10.0.0.0***

Router1(config-router)#**exit**

Router1(config)#**username *dialhost* password *cisco***

Router1(config)#**access-list *101* deny eigrp any any**

Router1(config)#**access-list *101* permit ip any any**

Router1(config)#**dialer-list *1* protocol ip list *101***

Router1(config)#**dialer watch-list *1* ip *10.2.0.0 255.255.0.0***

Router1(config)#**dialer watch-list *1* ip *10.1.1.0 255.255.255.0***

Router1(config)#**dialer watch-list *1* delay route-check initial *300***

Router1(config)#**dialer watch-list *1* delay disconnect *15***

Router1(config)#**end**

Router1#

注释 Dialer Watch 通过跟踪路由表中特定路由前缀的存在情况来判断是否需要触发拨号，这里要特别注意的是例子中监控了两个路由前缀，必须两个路由前缀都消失才会触发拨号。还是建议使用 13.1 中的浮动路由方式来进行拨号备份

13.6. 使用 VIRTUAL TEMPLATES

提问 使用 Virtual Templates 的方式来配置拨号备份

回答

```
dialhost#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
dialhost(config)#username Router1 password dialpassword
dialhost(config)#interface BRI0/0
dialhost(config-if)#no ip address
dialhost(config-if)#encapsulation ppp
dialhost(config-if)#dialer pool-member 1
dialhost(config-if)#isdn switch-type basic-ni
dialhost(config-if)#isdn point-to-point-setup
dialhost(config-if)#isdn spid1 800555123400 5551234
dialhost(config-if)#isdn spid2 800555123500 5551235
dialhost(config-if)#ppp authentication chap
dialhost(config-if)#ppp multilink
dialhost(config-if)#exit
dialhost(config)#interface Dialer1
dialhost(config-if)#no ip address
dialhost(config-if)#encapsulation ppp
dialhost(config-if)#dialer idle-timeout 300
dialhost(config-if)#dialer-group 1
dialhost(config-if)#no peer default ip address
dialhost(config-if)#ppp authentication chap
dialhost(config-if)#ppp multilink
```

dialhost(config-if)#**exit**

dialhost(config)#**access-list *101* deny eigrp any any**

dialhost(config)#**access-list *101* permit ip any any**

dialhost(config)#**dialer-list *1* protocol ip list *101***

dialhost(config)#**router eigrp *55***

dialhost(config-router)#**network *10.0.0.0***

dialhost(config-router)#**exit**

dialhost(config)#**interface *Loopback1***

dialhost(config-if)#**ip address *10.1.99.1 255.255.255.0***

dialhost(config-if)#**exit**

dialhost(config)#**interface Virtual-Template*1***

dialhost(config-if)#**ip unnumbered *Loopback1***

dialhost(config-if)#**encapsulation *ppp***

dialhost(config-if)#**ppp authentication chap**

dialhost(config-if)#**ppp multilink**

dialhost(config-if)#**ppp multilink load-threshold *50* either**

dialhost(config-if)#**exit**

dialhost(config)#**virtual-profile virtual-template *1***

dialhost(config)#**end**

dialhost#

注释 一般用于中心的拨号服务器，类似于 13.2 但是在 Dialer 接口下也没有配置 IP 地址，而是配置在 Virtual Template 上

13.7. 确保断线正常

提问 当主链路恢复以后确保备份链路断线正常

回答

```
Router1#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router1(config)#interface Serial0/0.1 point-to-point
Router1(config-subif)#bandwidth 56
Router1(config-subif)#exit
Router1(config)#interface BRI0/0
Router1(config-subif)#bandwidth 54
Router1(config-subif)#end
Router1#
```

注释 通过配置带宽的方式来调整主备接口的 metric 值，从而避免在路由计算时选用备份接口

13.8. 查看拨号备份状态

提问 查看拨号备份状态

回答

```
Router1#show dialer
Router1#show backup
Router1#show isdn status
Router1#show isdn active
Router1#show isdn history
```

注释 show dialer 里面比较有意思的信息是 Dial reason: ip (s=10.1.99.55, d=224.0.0.10)，从而确定是什么数据触发的拨号

13.9. 拨号备份排错

提问 查找拨号备份失败原因

回答

Router1#**debug ppp authentication**

Router1#**debug dialer**

注释 无

第十四章 NTP 和时间

14.1. 路由器日志显示时间戳

提问 在路由器的日志和排错信息里面显示时间

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**service timestamps log datetime localtime**

Router(config)#**service timestamps debug datetime localtime**

Router(config)#**end**

Router#

注释 还可以在命令后面加上 show-timezone, msec 等参数让时间戳包含时区信息和毫秒级

14.2. 设置时间

提问 设置路由器时间

回答

内部时钟

Router#**clock set *14:27:22 January 29 2006***

Router#

高端路由器使用电池保存时间

Router#**calendar set *14:34:39 January 29 2006***

Router#

注释 如果没有电池保护路由器重启时间配置消失，show calendar 一方面可以显示目前时钟，也可以用来验证是否有电池保护，内部时钟和 calendar 时钟不一致时可以使用 **clock update-calendar** 或者 **clock read-calendar** 来互相同步

14.3. 设置时区

提问 设置路由器时区

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**clock timezone *EST 5***

Router(config)#**end**

Router#

注释 缺省路由器使用 UTC 就是以前的 GMT

14.4. 夏时制调整

提问 路由器自动对时钟进行夏时制调整

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**clock summer-time *EDT* date *26 oct 2003 02:00 6 apr 2003 02:00***

或者

Router(config)#**clock summer-time *AEDT* recurring last *sun oct 02:00 last sun mar 02:00***

Router(config)#**end**

Router#

注释 缺省是没有夏时制的，启用后可以使用 show clock detail 来验证

14.5. 时钟同步(NTP)

提问 路由器自动同步网络时间

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**clock timezone *EST -5***

Router(config)#**clock summer-time *EDT* recurring**

Router(config)#**ntp server *172.25.1.1***

Router(config)#**end**

Router#

对于不支持 NTP 的路由器，使用 SNTP

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**clock timezone *EST -5***

Router(config)#**clock summer-time *EDT* recurring**

Router(config)#**sntp server *172.25.1.1***

Router(config)#**end**

Router#

注释 可以使用 **ntp source *loopback0*** 或者 **ntp server *10.1.1.1* source *Serial 0/0*** 命令来指定 NTP 发送的源地址。由于 NTP 同步的是内部时钟，所以需要配置 **ntp update-calendar** 来同时同步其 calendar 时钟

14.6. 配置 NTP 冗余

提问 配置多个 NTP 服务器的方式来提供冗余

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**clock timezone *EST -5***

Router(config)#**clock summer-time *EDT* recurring**

Router(config)#**ntp server *172.25.1.1***

Router(config)#**ntp server *10.121.33.231***

Router(config)#**ntp peer *192.168.12.12***

Router(config)#**end**

Router#

注释 无

14.7. 设置路由器为网络 NTP 服务器

提问 设置路由器为网络 NTP 服务器，成为网络的主时钟源

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**clock timezone *EST 5***

Router(config)#**clock summer-time *EDT* recurring**

Router(config)#**clock calendar-valid**

Router(config)#**ntp master *8***

Router(config)#**end**

Router#

注释 这里设置 ntp master 8 使其成为 Stratum level 8，尽量不要配置其为 1

14.8. 调整 NTP 同步周期

提问 调整多久路由器发送 NTP 数据包来验证同步

回答

NTP 不允许手动修改同步频率，但是内置的算法可以自动调整此频率

注释 开始为 64 秒一个周期，如果网络足够稳定此周期会逐渐增加，最长到 1024 秒，如下例

Router>**show ntp associations**

```
      address         ref clock      st   when   poll reach  delay  offset    disp
*~172.25.1.1       130.207.244.240    2    440   1024   377     1.6    -3.23     5.6
+~172.25.1.3       204.152.184.72     2    829   1024   377     1.7     8.06     0.9
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

```
Router>
```

14.9. NTP 发送周期性广播包保持更新

提问 工作于广播模式下，不需要周期性去查询

回答

服务器端

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**clock timezone** EST -5

Router1(config)#**clock summer-time** EDT **recurring**

Router1(config)#**ntp server** 172.25.1.1

Router1(config)#**ntp server** 172.25.1.2

Router1(config)#**interface** FastEthernet0/0

Router1(config-if)#**ntp broadcast**

Router1(config-if)#**end**

Router1#

客户端

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**clock timezone** ***EST -5***

Router2(config)#**clock summer-time** ***EDT*** **recurring**

Router2(config)#**ntp broadcastdelay** ***4***

Router2(config)#**interface *Ethernet0***

Router2(config-if)#**ntp broadcast client**

Router2(config-if)#**end**

Router2#

注释 工作于广播模式时间数据包是单方向的，通过 broadcastdelay 来控制周期，广播模式不妨碍客户端工作于服务器客户端模式

14.10. NTP 发送周期性组播包保持更新

提问 工作于组播模式下，不需要周期性去查询

回答

服务器端

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**clock timezone *EST -5***

Router1(config)#**clock summer-time *EDT* recurring**

Router1(config)#**ntp server *172.25.1.1***

Router1(config)#**ntp server *172.25.1.3***

Router1(config)#**interface *FastEthernet 0/0***

Router1(config-if)#**ntp multicast *224.0.1.1* ttl *1***

Router1(config-if)#**end**

Router1#

客户端

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**clock timezone** ***EST -5***

Router1(config)#**clock summer-time** ***EDT*** **recurring**

Router1(config)#**ntp server** ***172.25.1.1***

Router1(config)#**ntp server** ***172.25.1.3***

Router1(config)#**interface** ***FastEthernet 0/0***

Router1(config-if)#**ntp multicast** ***224.0.1.1*** **ttl** ***1***

Router1(config-if)#**end**

Router1#

注释 组播相对于广播的好处不用多说了，并且在这个模式的初始客户端会先发送一些单播包来测量延迟，以使时间更准确，需要注意的是不是所有的设备都支持这种组播模式

14.11. 基于接口开启 NTP

提问 路由器配置为 NTP 服务器，但是某些端口禁止 NTP 服务

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**interface** ***Serial0/1***

Router(config-if)#**ntp disable**

Router(config-if)#**end**

Router#

或者

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**access-list *107* deny udp any eq 123 any eq 123**

Router(config)#**access-list *107* permit ip any any**

Router(config)#**interface *Serial0/1***

Router(config-if)#**ip access-group *107* in**

Router(config-if)#**end**

Router#

注释 控制列表的方式更严格，第一种只是阻止了相应的 associations，但阻止不了 NTP 数据包

14.12. NTP 认证

提问 鉴权 NTP 数据包保证安全

回答

服务器端

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ntp authentication-key *2* md5 *neoshi***

Router1(config)#**ntp authenticate**

Router1(config)#**ntp trusted-key *2***

Router1(config)#**end**

Router1#

客户端

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**ntp authentication-key *2* md5 *neoshi***

Router2(config)#**ntp authenticate**

Router2(config)#**ntp trusted-key *2***

Router2(config)#**ntp server *172.25.1.5* key *2***

Router2(config)#**end**

Router2#

注释 对于广播或者组播模式 key 配置为 ntp broadcast key 2 和 ntp multicast key 2

14.13. 限制 NTP PEERS 数目

提问 限制路由器可以接受的 NTP Peers 的数目

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**ntp max-associations *30***

Router(config)#**end**

Router#

注释 无

14.14. 限制 PEERS

提问 对 NTP 服务进行更好粒度的控制

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**access-list *88* permit host *172.25.1.1***

Router(config)#**access-list *88* permit host *10.1.1.1***

Router(config)#**access-list *99* permit *172.25.0.0 0.0.255.255***

Router(config)#**access-list *99* permit *10.2.0.0 0.0.255.255***

Router(config)#**clock timezone *EST -5***

Router(config)#**clock summer-time *EDT* recurring**

Router(config)#**ntp server *172.25.1.1* version *3***

Router(config)#**ntp server *10.1.1.1* version *3***

Router(config)#**ntp access-group peer *88***

Router(config)#**ntp access-group serve-only *99***

Router(config)#**end**

Router#

注释 路由器只允许内部时钟从 ACL88 定义的两个服务器中获的同步，同时只有 ACL99 定义的两个网段的客户端可以从本设备请求时间信息

14.15. 设定时钟周期

提问 希望调整自动生成的 *ntp clock-period xxxxxx* 数值

回答

路由器在重启之后会自动生成一个时钟周期来加速再同步，不建议删除或者修改

Router#**show running-config | include clock-period**

ntp clock-period 17180200

Router#

注释 无

14.16. 检查 NTP 状态

提问 查看当前 NTP 状态

回答

Router>**show clock detail**

Router>**show ntp status**

Router>**show ntp associations**

Router>**show ntp associations detail**

注释 Router>**show clock detail**

.15:54:33.079 EST Sun Jan 29 2006

Time source is NTP

此输出前面有个.代表此时钟没有同步

14.17. NTP 排错

提问 解决 NTP 出错的问题

回答

NTP 非常稳定，出问题很大可能性就是连接性的问题

Router#**debug ntp packets**

注释 Router#**debug ntp packet**

NTP packets debugging is on

.Mar 21 02:39:18: **NTP: xmit packet to 172.25.1.5**:

.Mar 21 02:39:18: leap 3, mode 3, version 3, **stratum 0**, ppoll 64

```
.Mar 21 02:39:18:    rtdel 28C7 (159.286), rtdsp 2444 (141.663), refid AC190101
.Mar 21 02:39:18:    ref C043C43F.47A9CD5C (21:30:23.279 EST Wed Mar 20 2003)
.Mar 21 02:39:18:    org 00000000.00000000 (19:00:00.000 EST Thu Dec 31 1899)
.Mar 21 02:39:18:    rec 00000000.00000000 (19:00:00.000 EST Thu Dec 31 1899)
.Mar 21 02:39:18:    xmt C043C656.4DFC7394 (21:39:18.304 EST Wed Mar 20 2003)
.Mar 21 02:39:25: NTP: rcv packet from 172.25.1.5 to 172.16.2.2 on Fa0/0.1:
.Mar 21 02:39:25:    leap 3, mode 3, version 3, stratum 0, ppoll 64
.Mar 21 02:39:25:    rtdel 286E (157.928), rtdsp 0EC6 (57.709), refid AC190101
.Mar 21 02:39:25:    ref C043C4D7.1D633CDE (21:32:55.114 EST Wed Mar 20 2003)
.Mar 21 02:39:25:    org 00000000.00000000 (19:00:00.000 EST Thu Dec 31 1899)
.Mar 21 02:39:25:    rec 00000000.00000000 (19:00:00.000 EST Thu Dec 31 1899)
.Mar 21 02:39:25:    xmt C043C65D.1D0A6CBC (21:39:25.113 EST Wed Mar 20 2003)
.Mar 21 02:39:25:    inp C043C65D.1296E3C7 (21:39:25.072 EST Wed Mar 20 2003)
```

上面是一个 debug 的输出，从中看到了来自 server 的数据包显示为 stratum 0，代表服务器没有同步，既然上游服务器没有同步，本地服务器就更不能同步了

14.18. NTP 日志

提问 记录重要的 NTP 事件

回答

```
Router2#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router2(config)#ntp logging
Router2(config)#end
```

Router2#

注释 此命令来自 12.3(7)T，下面是一个日志记录

Router2#**show logging | include NTP**

000019: Jan 29 10:57:52.633 EST: %NTP-5-PEERSYNC: NTP synced to peer 172.25.1.5

000020: Jan 29 10:57:52.637 EST: %NTP-6-PEERREACH: Peer 172.25.1.5 is reachable

000024: Jan 29 11:01:20.653 EST: %NTP-4-PEERUNREACH: Peer 172.25.1.5 is unreachable

000026: Jan 29 11:15:11.985 EST: %NTP-4-UNSYNC: NTP sync is lost

14.19. 扩展夏时制（EXTENDED DAYLIGHT SAVING TIME）

注释 美国为了节省能源从 2007 年开始调整了夏时制的设置，此略去

14.20. NTP 服务器配置

注释 主机配置暂略去

第十五章 DLSW

略去

第十六章 路由器接口

16.1. 查看接口状态

提问 查看当前路由器接口状态

回答

Router1#**show interfaces**

Router1#**show interfaces *FastEthernet0/1***

Router1#**show ip interface brief**

Router1#**show ip interface *FastEthernet0/1***

注释 show interface 命令的输出有很多的信息，网上一些中文文档详细介绍输出的含义，这里不翻译了。Txload 和 rxload 这两个测量值的周期缺省是 5 分钟，可以使用 **load-interval** ***60*** 命令来修改其为 60 秒，必须是 30 的倍数，最长 10 分钟。再来一个隐藏命令

Router1#**show interfaces *FastEthernet0/1* stats**

FastEthernet0/1

Switching path	Pkts In	Chars In	Pkts Out	Chars Out
Processor	294567	18704930	239526	22219870
Route cache	7758	681257	48303	6129834
Total	302325	19386187	287829	28349704

Processor 是 process switching，Route cache 是 Fast Switching

16.2. 配置串行接口

提问 为广域网连接配置串行接口

回答

Router3#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router3(config)#**interface *Serial1***

Router3(config-if)#**description *WAN Connection to Chicago***

Router3(config-if)#**ip address *192.168.99.5 255.255.255.252***

Router3(config-if)#**encapsulation *hdlc***

Router3(config-if)#**clock rate *56000***

Router3(config-if)#**no shutdown**

Router3(config-if)#**exit**

Router3(config)#**end**

Router3#

注释 在 DCE 侧需要配置 clock rate，如果是 DTE 配置了 clock rate 路由器会忽略此配置。通过 show controller serial 命令来判断连接线缆的类型。缺省情况路由器会认为串口为 1.544M 带宽，而实际可能不是，为了准确进行路由协议度量值计算，需要人工 bandwidth 命令来修改，注意这里的单位是 Kilobits 每秒，而 clock rate 是 bits 每秒

16.3. 使用内置 T1 CSU/DSU

提问 使用内置 T1 CSU/DSU 配置广域网连接

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *Serial0/1***

Router1(config-if)#**ip address *192.168.99.9 255.255.255.252***

Router1(config-if)#**no shutdown**

Router1(config-if)#**service-module t1 timeslots *1-12***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 缺省每个 channel 使用 64Kbps，如果电路是 56k 的需要在上述 service module 命令后面加上 speed 56。还有很多的参数，需要和对端一致

Router1(config-if)#**service-module t1 linecode ami**

Router1(config-if)#**service-module t1 data-coding inverted**

Router1(config-if)#**service-module t1 framing sf**

Router1(config-if)#**service-module t1 fdl ansi**

Router1(config-if)#**service-module t1 fdl att**

Router1(config-if)#**service-module t1 remote-alarm-enable**

通常运营商会提供时钟，如果在实验网络需要其成为 DCE 需要配置 **service-module t1 clock source internal** 来提供时钟

16.4. 使用内置 ISDN PRI 模块

提问 配置内置 ISDN PRI 模块

回答

Router8#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router8(config)#**isdn switch-type primary-dms100**

Router8(config)#**controller T1 0**

Router8(config-controlle)#**framing esf**

Router8(config-controlle)#**clock source line primary**

Router8(config-controlle)#**linecode b8zs**

Router8(config-controlle)#**pri-group timeslots *1-24***

Router8(config-controlle)#**exit**

Router8(config)#**end**

Router8#

注释 无

16.5. 使用内置 56 KBPS CSU/DSU

提问 配置内置 56 Kbps CSU/DSU

回答

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**interface *Serial0/1***

Router2(config-if)#**ip address *192.168.99.25 255.255.255.252***

Router2(config-if)#**no shutdown**

Router2(config-if)#**service-module 56k clock rate *9.6***

Router2(config-if)#**exit**

Router2(config)#**end**

Router2#

注释 这种模块没有见过，有点晕，先略一下

16.6. 配置异步串行接口

提问 配置一个同步/异步串行接口工作于异步模式

回答

Router3#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router3(config)#**interface *Serial1/7***

Router3(config-if)#**physical-layer async**

Router3(config-if)#**encapsulation ppp**

Router3(config-if)#**exit**

Router3(config)#**line *40***

Router3(config-line)#**speed *115200***

Router3(config-line)#**exit**

Router3(config)#**end**

Router3#

注释 在配置了 physical-layer async 命令以后需要查看 line 号

Router3#show line

Tty	Typ	Tx/Rx	A	Modem	Roty	AccO	AccI	Uses	Noise	Overruns	Int
0	CTY		-	-	-	-	-	0	0	0/0	-
40	TTY	9600/9600	-	-	-	-	-	0	0	0/0	Se1/7
65	AUX	2400/2400	F	-	-	-	-	0	0	0/0	-

看到 Se1/7 为 line 40，同时其速率变为 9600，所以需要使用 speed 命令来修改速率

16.7. 配置 ATM 子接口

提问 基于 PVC 的 ATM 链路互联

回答

老方法

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**interface ATM*0/0***

Router2(config-if)#**no ip address**

Router2(config-if)#**exit**

Router2(config)#**interface ATM*0/0.1* point-to-point**

Router2(config-subif)#**description *PVC to New York***

Router2(config-subif)#**ip address *192.168.250.146 255.255.255.252***

Router2(config-subif)#**atm pvc *1 0 60* aal5snap *10000 5000 3* oam *5***

Router2(config-subif)#**exit**

Router2(config)#**end**

Router2#

11.3 以后使用思科特性周期性发送 ATM OAM 信元来测试 VC

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**interface ATM*0/0***

Router2(config-if)#**no ip address**

Router2(config-if)#**exit**

Router2(config)#**interface ATM*0/0.1* point-to-point**

Router2(config-subif)#**description *PVC to New York***

Router2(config-subif)#**ip address *192.168.250.146 255.255.255.252***

Router2(config-subif)#**pvc *0/60***

Router2(config-if-atm-vc)#**vbr-nrt *10000 5000 30***

Router2(config-if-atm-vc)#**oam-pvc manage *5***

Router2(config-if-atm-vc)#**exit**

Router2(config)#**end**

Router2#

注释 第一种方法验证 Router2#**show atm pvc *0/60***

ATM0/0.1: VCD: 1, VPI: 0, VCI: 60, etype:0x0, AAL5 - LLC/SNAP, Flags: 0x830

PeakRate: 10000, Average Rate: 5000, Burst Cells: 96, VCmode: 0xE000

OAM frequency: 5 second(s), InARP frequency: 15 minute(s)

InPkts: 1292959637, OutPkts: 3327374998, InBytes: 2196038015, OutBytes: 813592646

InPRoc: 19959239, OutPRoc: 24660, Broadcasts: 19481389

InFast: 1212924649, OutFast: 3297025318, InAS: 60075750, OutAS: 10843631

OAM F5 cells sent: 6804133, OAM cells received: 6740056

Status: ACTIVE

VCD 是本地有效，VPI VCI 必须和对端相同，至于封装协议推荐是 AAL5SNAP，如果需要支持 PPP 则改为 AAL5CISCOPPP

在新方法里面已经没有配置 VCD 了，并且如果 3 个 OAM 信元没有收到就会标记此接口断掉，在 12.2(4)T 后还引入了 Router2(config)#**snmp-server enable traps atm pvc extension oam failure loopback** 来支持 SNMP 告警

16.8. 设置有效载荷绕码（PAYLOAD SCRAMBLING）

提问 设置有效载荷绕码

回答

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**interface ATM*0/0***

Router2(config-if)#**atm ds3-scramble** （**atm e3-scramble**）

Router2(config-if)#**exit**

Router2(config)#**end**

Router2#

Router4#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router4(config)#**interface ATM*0/0***

Router4(config-if)#**atm scrambling cell-payload**

Router4(config-if)#**exit**

Router4(config)#**end**

Router4#

注释 暂略

16.9. 传统的 ATM 承载 IP（CLASSICAL IP OVER ATM）

提问 配置路由器支持 SVC 和传统的 ATM 承载 IP

回答

首先 ATMARP Server

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface ATM*1/0***

Router1(config-if)#**no ip address**

Router1(config-if)#**atm ilmi-keepalive**

Router1(config-if)#**pvc 0/5 qsaal**

Router1(config-if-atm-vc)#**exit**

Router1(config-if)#**pvc 0/16 ilmi**

Router1(config-if-atm-vc)#**exit**

Router1(config-if)#**exit**

Router1(config)#**interface ATM*1/0.1* multipoint**

Router1(config-subif)#**ip address *192.168.123.1 255.255.255.0***

Router1(config-subif)#**atm esi-address *A000C0A87B01.01***

Router1(config-subif)#**atm arp-server self**

Router1(config-subif)#**exit**

Router1(config)#**end**

Router1#

其他 Client

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**interface ATM*1/0***

Router2(config-if)#**no ip address**

Router2(config-if)#**atm ilmi-keepalive**

Router2(config-if)#**pvc 0/5 qsaal**

Router2(config-if-atm-vc)#**exit**

Router2(config-if)#**pvc 0/16 ilmi**

Router2(config-if-atm-vc)#**exit**

Router2(config-if)#**exit**

Router2(config)#**interface ATM*1/0.1* multipoint**

Router2(config-subif)#**ip address *192.168.123.2 255.255.255.0***

Router2(config-subif)#**atm esi-address *A000C0A87B02.01***

Router2(config-subif)#**atm arp-server nsap** ***47.00918100000000e014cd0001.A000C0A87B01.01***

Router2(config-subif)#**exit**

Router2(config)#**end**

Router2#

注释 除了上面的使用 ATM SVC 以外，还有 Local Area Network Emulation (LANE)和 Multiple Protocols over ATM (MPOA)也支持，都是解决 Quasi Signaling Application Adaptation Layer (QSAAL) 协议和 nterim Local Management Interface (ILMI)的问题。在客户机配置 arp 服务器的地址要记的加上前缀，并不仅仅是服务器的 ESI 地址

16.10. 配置以太网接口特性

提问 对以太网接口的速率，双工等特性进行配置

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface FastEthernet0/0**

Router1(config-if)#**media-type 100BaseX**

Router1(config-if)#**duplex full**

Router1(config-if)#**speed 100**

Router1(config-if)#**mac-address** ***0AAA.ABCD.0101***

Router1(config-if)#**arp timeout** ***60***

Router1(config-if)#**keepalive** ***5***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 无

16.11. 配置令牌环接口特性

提问 配置令牌环接口

回答

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**interface TokenRing0**

Router2(config-if)#**ring-speed *4***

Router8(config-if)#**full-duplex**

Router2(config-if)#**mac-address *0006.1111.aaaa***

Router2(config-if)#**exit**

Router2(config)#**end**

Router2#

注释 不是所有的令牌环模块都支持全双工

16.12. 使用 ISL 协议配置 VLAN TRUNKS

提问 使用 ISL 协议配置 Vlan Trunks

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface FastEthernet0/0**

Router1(config-if)#**no ip address**

Router1(config-if)#**speed 100**

Router1(config-if)#**full-duplex**

Router1(config-if)#**exit**

Router1(config)#**interface FastEthernet0/0.1**

Router1(config-subif)#**encapsulation isl 1**

Router1(config-subif)#**ip address *172.25.1.5 255.255.255.0***

Router1(config-subif)#**exit**

Router1(config)#**interface FastEthernet0/0.2**

Router1(config-subif)#**encapsulation isl 2**

Router1(config-subif)#**ip address *172.16.2.1 255.255.255.0***

Router1(config-subif)#**exit**

Router1(config)#**interface FastEthernet0/0.3**

Router1(config-subif)#**encapsulation isl 574**

Router1(config-subif)#**ip address *10.22.1.2 255.255.255.0***

Router1(config-subif)#**exit**

Router1(config)#**end**

Router1#

注释 通常所说的单臂路由，ISL 是思科特有的

Router1#**show interfaces *FastEthernet0/0.3***

Encapsulation ISL Virtual LAN, Color 574.

在 12.2(4)T 以后增加了

Router1(config)#**interface *FastEthernet0/0.1***

Router1(config-if)#**ip unnumbered *Loopback0***

16.13. 使用 802.1Q 协议配置 VLAN TRUNKS

提问 使用 802.1Q 协议配置 Vlan Trunks

回答

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**interface FastEthernet1/0**

Router2(config-if)#**no ip address**

Router2(config-if)#**speed 100**

Router2(config-if)#**full-duplex**

Router2(config-if)#**exit**

Router2(config)#**interface FastEthernet1/0.1**

Router2(config-subif)#**encapsulation dot1Q 1 native**

Router2(config-subif)#**ip address *172.25.1.47 255.255.255.0***

Router2(config-subif)#**exit**

Router2(config)#**interface FastEthernet1/0.2**

Router2(config-subif)#**encapsulation dot1Q 2**

Router2(config-subif)#**ip address *172.25.22.4 255.255.255.0***

Router2(config-subif)#**exit**

Router2(config)#**interface FastEthernet1/0.3**

Router2(config-subif)#**encapsulation dot1Q 548**

Router2(config-subif)#**ip address *172.20.1.1 255.255.255.0***

Router2(config-subif)#**exit**

Router2(config)#**end**

Router2#

注释 这里面要注意的是 native vlan 的配置，缺省是 vlan 1，但是也可以设定为其他的，要保证路由器的 native vlan 和交换机的是一致的

16.14. LPD 打印机支持

提问 把打印机接到路由器的异步串行口上

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**printer *rtlpr1* line *161***

Router1(config)#**end**

Router1#

注释 首先要有一台主机支持 Berkeley Unix LPD print program，然后配置主机 *etc/printcap* 把打印工作转到路由器，然后你的打印机要支持串口连接，最后通过 show line 的命令找到 AUX 端口的 line 号，也就是上例子中的 161，同时建议下面配置

Router1(config)#**line aux *0***

Router1(config-line)#**no exec**

Router1(config-line)#**no login**

Router1(config-line)#**no password**

Router1(config-line)#**transport input none**

Router1(config-line)#**speed *115200***

Router1(config-line)#**exit**

Router1#**show printer**

Printer Line Rotary Errors Connections Datafiles Controlfiles Bytes

rtlpr1 161 0 0 0 0 0 0

Router1#

第十七章 SNMP

17.1. 配置 SNMP

提问 在路由器上启用基本的 SNMP 服务

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**snmp-server community *ORARO* ro**

Router(config)#**snmp-server community *ORARW* rw**

Router(config)#**end**

Router#

从 12.0 以后启用了另一种配置方式

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**snmp-server group *COOKRO* v1**

Router(config)#**snmp-server user *TESTRO1 COOKRO* v1**

Router(config)#**snmp-server group *BOOKRO* v2c**

Router(config)#**snmp-server user *TESTRO2 BOOKRO* v2c**

Router(config)#**end**

注释 注意的是这里启用的仅仅是简单 SNMP 服务，只会响应 SNMP 的 GET 和 SET 请求，不会发送 SNMP traps informs.由于 SNMP V1 和 V2c 都是明文传输 community 值所以需要后续的一些安全限制。**show snmp group** 可以用来验证

17.2. 通过 SNMP 工具获的路由器信息

注释 可以使用 snmpget， snmpwalk，snmpset 命令直接对 MIB 进行查询，建议使用 Solarwinds 等图形化工具，暂略。

思科 MIBs 信息：http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

17.3. 为 SNMP 访问配置一些路由器重要信息

提问 为 SNMP 访问提供类似路由器位置，序列号等重要信息

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**snmp-server contact *Ian Brown 416-555-2943***

Router(config)#**snmp-server location *999 Queen St. W., Toronto, Ont.***

Router(config)#**snmp-server chassis-id *JAX123456789***

Router(config)#**end**

Router#

注释 无

17.4. 使用 SNMP 获的批量路由设备信息

注释 使用 perl 脚本来进行批量化操作，暂略

17.5. 使用控制列表来限制 SNMP 访问

提问 使用控制列表的方式来提高 SNMP 访问的安全性

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**access-list *99* permit *172.25.1.0 0.0.0.255***

Router(config)#**access-list *99* permit host *10.1.1.1***

Router(config)#**access-list *99* deny any**

Router(config)#**snmp-server community *ORARO* ro *99***

Router(config)#**access-list *98* permit *172.25.1.0 0.0.0.255***

Router(config)#**snmp-server community *ORARW* rw *98***

Router(config)#**end**

Router#

SNMP Group 的方法

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**access-list *99* permit *172.25.1.0 0.0.0.255***

Router(config)#**access-list *99* permit host *10.1.1.1***

Router(config)#**access-list *99* deny any**

Router(config)#**snmp-server group *COOKRO* v1 access *99***

Router(config)#**snmp-server user *TESTRO1 COOKRO* v1**

Router(config)#**end**

Router#

从 12.3(2)T 以后支持命名控制列表

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**ip access-list standard *SNMPACL***

Router2(config-std-nacl)#**permit *172.25.1.0 0.0.0.255***

Router2(config-std-nacl)#**permit host *10.1.1.1***

Router2(config-std-nacl)#**deny any**

Router2(config-std-nacl)#**snmp-server community *ORARO1* ro *SNMPACL***

Router2(config)#**end**

Router2#

注释 无

17.6. 记录非授权的 SNMP 尝试

提问 对非授权的 SNMP 尝试进行日志记录

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**access-list *99* permit *172.25.1.0 0.0.0.255***

Router(config)#**access-list *99* permit host *10.1.1.1***

Router(config)#**access-list *99* deny any log**

Router(config)#**snmp-server community *ORARO* ro *99***

Router(config)#**snmp-server community *ORARW* rw *99***

Router(config)#**end**

Router#

注释 Router#**show access-list *99***

Standard IP access list 99

permit 10.1.1.1 (1293 matches)

permit 172.25.1.0, wildcard bits 0.0.0.255 (630 matches)

deny any **log** (17 matches)

Router#**show logging**

Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)

Console logging: disabled

Monitor logging: level debugging, 26 messages logged

Logging to: vty2(0)

Buffer logging: level debugging, 49 messages logged

Trap logging: level informational, 53 message lines logged

Logging to 172.25.1.1, 53 message lines logged

Logging to 172.25.1.3, 53 message lines logged

Log Buffer (4096 bytes):

Apr 15 22:33:21: %SEC-6-IPACCESSLOGS: list 99 denied 192.168.22.13 1 packet

Apr 15 22:39:18: %SEC-6-IPACCESSLOGS: list 99 denied 10.121.212.11 3 packets

Router#

17.7. 限制 MIB 访问

提问 限制特定的 MIB 可以被 SNMP 来访问

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**access-list *99* permit *172.25.1.0 0.0.0.255***

Router(config)#**access-list *99* deny *any* log**

Router(config)#**snmp-server view *ORAVIEW* mib-2 included**

Router(config)#**snmp-server view *ORAVIEW* at excluded**

Router(config)#**snmp-server view *ORAVIEW* cisco included**

Router(config)#**snmp-server community *ORARO* view *ORAVIEW* ro *99***

Router(config)#**snmp-server view *RESTRICTED lsystem.55* included**

Router(config)#**snmp-server community *ORARW* view *RESTRICTED* rw *99***

Router(config)#**end**

Router#

SNMP Group 方式

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**snmp-server view *ORAVIEW* mib-2 included**

Router(config)#**snmp-server view *ORAVIEW* at excluded**

Router(config)#**snmp-server view *ORAVIEW* cisco included**

Router(config)#**snmp-server group *TEST* v1 read *ORAVIEW***

Router(config)#**snmp-server user** ***ORARO TEST*** **v1**

Router(config)#**snmp-server view** ***RESTRICTED lsystem.55*** **included**

Router(config)#**snmp-server group** ***TEST2*** **v1 write** ***RESTRICTED***

Router(config)#**snmp-server user** ***ORARW TEST2*** **v1**

Router(config)#**end**

Router#

注释

Router#**show snmp view**

ORAVIEW mib-2 - included nonvolatile active

ORAVIEW at - excluded nonvolatile active

ORAVIEW cisco - included nonvolatile active

v1default internet - included volatile active

v1default internet.6.3.15 - excluded volatile active

v1default internet.6.3.16 - excluded volatile active

v1default internet.6.3.18 - excluded volatile active

RESTRICTED cisco - included nonvolatile active

RESTRICTED lsystem.55 - included nonvolatile active

Router#

17.8. 使用 SNMP 来修改路由器当前配置

提问 使用 SNMP 来下载或者上传路由器配置文件

回答

以安装了 NETSNMP 的 Freebsd 为例

首先路由器启用 SNMP

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**snmp-server community *ORARW* rw**

Router(config)#**end**

下载配置

Freebsd% **touch */tftpboot/router.cfg***

Freebsd% **chmod 666 */tftpboot/router.cfg***

Freebsd% **snmpset v1 -c *ORARW Router* .1.3.6.1.4.1.9.2.1.55.*172.25.1.1* s *router.cfg***

enterprises.9.2.1.55.172.25.1.1 = "router.cfg"

Freebsd%

修改配置后上传保存

Freebsd% **echo "*no ip source-route*" > */tftpboot/new.cfg***

Freebsd% **echo "end" >> */tftpboot/new.cfg***

Freebsd% **chmod *666 /tftpboot/new.cfg***

Freebsd% **snmpset v1 -c *ORARW Router* .1.3.6.1.4.1.9.2.1.53.*172.25.1.1* s *new.cfg***

enterprises.9.2.1.53.172.25.1.1 = "new.cfg"

Freebsd% **snmpset v1 -c *ORARW Router* .1.3.6.1.4.1.9.2.1.54.0 i 1**

enterprises.9.2.1.54.0 = 1

Freebsd%

注释 .1.3.6.1.4.1.9.2.1.55 是思科 MIB 中发送当前配置文件的 OID 值，172.25.1.1 是 TFTP 服务器地址。在修改配置文件时候注意最后要加上 end 命令，注意这时的 OID 是.1.3.6.1.4.1.9.2.1.53。最后一个 snmpset 命令是对上传配置进行保存。当然上述操作都可以使用 Solarwinds 软件实现

17.9. 使用 SNMP 来升级 IOS

提问 通过 SNMP 来远端升级路由器 IOS

回答

首先路由器配置

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**snmp-server community *ORARW* rw**

Router(config)#**end**

下载当前的 IOS

Freebsd% **touch */tftpboot/c2600-jk9o3s-mz.122-7a.bin***

Freebsd% **chmod 666 */tftpboot/c2600-jk9o3s-mz.122-7a.bin***

Freebsd% **snmpset v1 -c *ORARW Router* .1.3.6.1.4.1.9.2.10.9.*172.25.1.1* s *c2600-jk9o3s-mz.122-7a.bin***

enterprises.9.2.10.9.172.25.1.1 = "c2600-jk9o3s-mz.122-7a.bin"

Freebsd%

升级 IOS

Freebsd% **chmod 666 */tftpboot/c2600-jk9o3s-mz.122-7a.bin***

Freebsd% **snmpset v1 -c *ORARW Router* .1.3.6.1.4.1.9.2.10.6.0 i 1**

enterprises.9.2.10.6.0 = 1

Freebsd% **snmpset v1 -c *ORARW Router*.**1.3.6.1.4.1.9.2.10.12.*172.25.1.1* s ***c2600-jk9o3s-mz.122-7a.bin***

enterprises.9.2.10.12.172.25.1.1 = "c2600-jk9o3s-mz.122-7a.bin"

Freebsd%

注释 例子中的 Router 是路由器的机器名也可以使用 IP 地址，.1.3.6.1.4.1.9.2.10.9.是相应的 OID。在对 IOS 升级的时候第一步做的是清除 Flash，第二步才是上传 IOS。这种可以使用脚本来实现 IOS 的集中管理。

17.10. 使用 SNMP 来进行批量的配置修改

注释 使用 perl 脚本来进行批量化操作，暂略

17.11. 避免非授权的配置修改

提问 只允许特定的设备来通过 SNMP 和 TFTP 来发送和接收配置信息

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**access-list *92* permit *172.25.1.1***

Router(config)#**access-list *92* deny any log**

Router(config)#**snmp-server tftp-server-list *92***

Router(config)#**snmp-server community *ORARW* rw**

Router(config)#**end**

Router#

从 12.3(2)T 开始支持命名控制列表

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**ip access-list standard *TFTPACL***

Router2(config-std-nacl)#**permit *172.25.1.1***

Router2(config-std-nacl)#**deny any log**

Router2(config-std-nacl)#**exit**

Router2(config)#**snmp-server tftp-server-list *TFTPACL***

Router2(config)#**snmp-server community *ORARW* rw**

Router2(config)#**end**

Router2#

注释 要注意的是这里限制的仅仅是通过 SNMP 发起的 TFTP 会话，对其他的文件传输不受影响。另外这里的控制列表是全局性的，不能针对特定的 community 值

17.12. 保持接口表名的永久性

提问 即使重启也能保证 SNMP 使用相同的接口名

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**snmp-server ifindex persist**

Router(config)#**end**

Router#

也可以对单独接口:

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**interface *Serial0/0***

Router(config-if)#**snmp ifindex persist**

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 很多工程师不知道内部 SNMP 接口号是会变的，这样在进行查询的时候会出错，比如下面的例子，FastEthernet1/0 的 ifindex 是 5

Freebsd% **snmpwalk v1 -c *ORARO Router* ifDescr**

interfaces.ifTable.ifEntry.ifDescr.1 = "BRI0/0"

interfaces.ifTable.ifEntry.ifDescr.2 = "Ethernet0/0"

interfaces.ifTable.ifEntry.ifDescr.3 = "BRI0/0:1"

interfaces.ifTable.ifEntry.ifDescr.4 = "BRI0/0:2"

interfaces.ifTable.ifEntry.ifDescr.5 = "FastEthernet1/0"

interfaces.ifTable.ifEntry.ifDescr.6 = "Null0"

interfaces.ifTable.ifEntry.ifDescr.7 = "Loopback0"

重启以后再查询就变成 2 了

Freebsd% **snmpwalk v1 -c *ORARO Router* ifDescr**

interfaces.ifTable.ifEntry.ifDescr.1 = "Ethernet0/0"

interfaces.ifTable.ifEntry.ifDescr.2 = "FastEthernet1/0"

interfaces.ifTable.ifEntry.ifDescr.3 = "Null0"

interfaces.ifTable.ifEntry.ifDescr.4 = "Loopback0"

这样就会给网管造成困难

17.13. 启用 SNMP TRAPS 和 INFORMS

提问 配置路由器针对特定事件产生 Traps 或者 Informs

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**snmp-server enable traps**

Router(config)#**snmp-server host *172.25.1.1 ORATRAP* config entity envmon hsrp**

Router(config)#**snmp-server host *nms.oreilly.com ORATRAP* bgp snmp envmon**

Router(config)#**end**

Router#

从 SNMP v2c 开始路由器支持 SNMP Informs

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**snmp-server enable informs**

Router(config)#**snmp-server host *172.25.1.1* informs version 2c *ORATRAP* snmp envmon**

Router(config)#**end**

Router#

注释 这里的 Traps 是路由器主动提供的，不是针对 SNMP request 的响应。可以 **snmp-server enable traps envmon** 来发送特定的 TRAPS，也可以针对不同的 NMS 主机发送不同的 traps

17.14. 以 SNMP TRAP 的形式发送 SYSLOG

提问 把 Syslog 封装成 SNMP Traps 或者 Informs

回答

Traps

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**logging history informational**

Router(config)#**snmp-server enable traps syslog**

Router(config)#**snmp-server host *172.25.1.1 ORATRAP* syslog**

Router(config)#**end**

Router#

Informs

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**logging history informational**

Router(config)#**snmp-server enable informs**

Router(config)#**snmp-server host *172.25.1.1* informs version 2c *ORATRAP* syslog**

Router(config)#**end**

Router#

注释 Router#**clear counters**

Clear "show interface" counters on all interfaces [confirm]

Router#

May 28 10:07:04: %CLEAR-5-COUNTERS: Clear counter on all interfaces by ijbrown on vty0 (172.25.1.1)

上述的 Syslog 信息会变成下面的 SNMP 消息

Freebsd% **tail snmptrapd.log**

May 28 10:07:04 freebsd snmptrapd[77759]: 172.25.25.1: Enterprise Specific Trap (1) Uptime: 18 days, 22:35:26.99, enterprises.9.9.41.1.2.3.1.2.118 = "CLEAR", enterprises.9.9.41.1.2.3.1.3.118 = 6,

enterprises.9.9.41.1.2.3.1.4.118 = "COUNTERS", enterprises.9.9.41.1.2.3.1.5.118 = "Clear counter on all interfaces by ijbrown on vty0 (172.25.1.1)", enterprises.9.9.41.1.2.3.1.6.118 = Timeticks: (163652698) 18 days, 22:35:26.98

Freebsd%

17.15. 设定 SNMP 包大小

提问 修改缺省的 SNMP 包大小

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**snmp-server packetsize *1480***

Router(config)#**end**

Router#

注释 缺省为 1500 字节

17.16. 设定 SNMP 队列大小

提问 增加 SNMP Trap 队列大小

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**snmp-server queue-length *25***

Router(config)#**snmp-server inform pending 40**

Router(config)#**end**

Router#

注释 缺省对 Trap 的队列是 10 个 trap 消息，对 Inform 是 25 个。可以通过 show snmp 来查看队列配置和丢弃的 Trap 包

17.17. 设定 SNMP 超时时长

提问 调整 SNMP Trap 的超时时长

回答

```
Router#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router(config)#snmp-server trap-timeout 60
Router(config)#snmp-server inform timeout 120
Router(config)#end
Router#
```

注释 准确说是重传等待时长

17.18. 禁止端口的 UP/DOWN TRAPS

提问 忽略特定端口的链路状态告警

回答

```
Router#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router(config)#interface Serial0/0
Router(config-if)#no snmp trap link-status
Router(config-if)#exit
Router(config)#end
Router#
```

注释 比如特定的拨号接口等

17.19. 设定 SNMP TRAPS 的源发送地址

提问 设定 SNMP Traps 消息的源发送地址

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**snmp-server host *172.25.1.1 ORATRAP***

Router(config)#**snmp-server trap-source *loopback0***

Router(config)#**end**

Router#

注释 无

17.20. 使用 RMON 来发送 TRAPS

提问 实现当 CPU 超过警戒后发送 trap 或者其他重要事件发送 trap

回答

CPU 超过特定阀值

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**rmon event 1 log trap *ORATRAP description "CPU on Router has exceeded threshold*" owner *ijbrown***

Router(config)#**rmon event 2 log description "*CPU on Router has normalized*" owner *ijbrown***

Router(config)#**rmon alarm 1 lsystem.57.0 60 absolute rising-threshold 70 1 falling-threshold *40* 2 owner *ijbrown***

Router(config)#**end**

Router#

内存利用超过特定阀值

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**rmon event 4 log trap *ORATRAP* description "*Low memory condition on Router*" owner *ijbrown***

Router(config)#**rmon event 5 log trap *ORATRAP description "Low Memory condition cleared on Router*" owner *ijbrown***

Router(config)#**rmon alarm 3 lsystem.8.0 60 absolute rising-threshold *1500000 5* falling-threshold *1000000 4* owner *ijbrown***

Router(config)#**end**

Router#

链路利用率超过固定阀值

er#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**rmon event 6 log trap *ORATRAP* description "*Bandwidth utilization has exceeded threshold on Router interface Serial 0/0*" owner *ijbrown***

Router(config)#**rmon event 7 log trap *ORATRAP* description "*Bandwidth utilization has normalized on Router interface Serial 0/0*" owner *ijbrown***

Router(config)#**! Configure inbound alarm on Serial0/0 (ifNumber 3)**

Router(config)#**rmon alarm 4 lifEntry.6.*3* 300 absolute rising-threshold *1000000 6* falling-threshold *800000 7* owner *ijbrown***

Router(config)#**! Configure outbound alarm on Serial0/0 (ifNumber 3)**

Router(config)#**rmon alarm 5 lifEntry.8.*3* 300 absolute rising-threshold *1000000 6* falling-threshold *800000 7* owner *ijbrown***

Router(config)#**end**

Router#

注释 路由器内置了这种廉价的监控方案

Router>**show rmon events**

Event 1 is active, owned by ijbrown

  Description is CPU on Router has exceeded threshold

  Event firing causes log and trap to community ORATRAP, last fired 00:00:00

Event 2 is active, owned by ijbrown

  Description is CPU on Router has normalized

  Event firing causes log, last fired 2w2d

  Current log entries:

        index   time   description

            1   2w2d   CPU on Router has normalized

Router>

17.21. 启用 SNMPV3

提问 启用 SNMPv3 提供安全性

回答

(*noAuthNoPriv*):

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**snmp-server view *TESTV3* mib-2 include**

Router(config)#**snmp-server group *NOTSAFE* v3 noauth read *TESTV3***

Router(config)#**snmp-server user *WEAK NOTSAFE* v3**

Router(config)#**end**

Router#

(*authNoPriv*):

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**snmp-server view *TESTV3* mib-2 include**

Router(config)#**snmp-server group *ORAROV3* v3 auth read *TESTV3***

Router(config)#**snmp-server user *cking ORAROV3* v3 auth md5** daytona19y

Router(config)#**end**

Router#

(*authPriv*)

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**snmp-server view *TESTV3* mib-2 include**

Router(config)#**snmp-server group *ORAROV3* v3 auth read *TESTV3***

Router(config)#**snmp-server user *bpugsley ORAROV3* v3 auth md5 *hockeyrules* priv des56 *shortguy***

Router(config)#**end**

Router#

注释 v3 最大的优点就是增加了安全性，有例子中三种模式可以选择

17.22. 高强度 SNMPV3 加密

提问 增强 V3 的加密

回答

从 12.4(2)T 开始增强了加密方法

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**snmp-server user *wbrejniak ORAROV3* v3 auth md5 *authpass* priv 3des *privpass***

Router1(config)#**end**

Router1#

或者

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**snmp-server user *wbrejniak ORAROV3* v3 auth md5 *authpass* priv aes 128 *privpass***

Router1(config)#**end**

Router1#

注释 无

17.23. 使用 SAA

提问 配置路由器自动轮询另一台设备来获的性能统计

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**rtr responder**

Router1(config)#**rtr *10***

Router1(config-rtr)#**type echo protocol ipIcmpEcho *10.1.2.3***

Router1(config-rtr)#**tag *ECHO_TEST***

Router1(config-rtr)#**threshold *1000***

Router1(config-rtr)#**frequency *300***

Router1(config-rtr)#**exit**

Router1(config)#**rtr schedule *10* life *2147483647* start-time now**

Router1(config)#**rtr *20***

Router1(config-rtr)#**type jitter dest-ipaddr *10.1.2.3* dest-port *99* num-packets *100***

Router1(config-rtr)#**tag *JITTER_TEST***

Router1(config-rtr)#**frequency *300***

Router1(config-rtr)#**exit**

Router1(config)#**rtr schedule *20* life *100000* start-time now ageout *3600***

Router1(config)#**exit**

Router1#

目标路由器，用来响应 SAA 测试

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**rtr responder**

Router2(config)#**exit**

Router2#

注释 无

第十八章 日志

18.1. 启用本地路由器日志

提问 实现路由器自身保存日志记录，而不仅仅是显示在终端上

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**logging buffered *informational***

Router(config)#**end**

Router#

注释 缺省日志记录为 debugging 级别，例子中为 informational 忽略掉了 debug 消息。禁用使用下面命令

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**no logging buffered**

Router(config)#**end**

Router#

18.2. 设定日志记录大小

提问 改变路由器保存日志记录的大小

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**logging buffered *16000***

Router(config)#**end**

Router#

注释 要注意的是改变了大小后，原有的日志记录会被清除。

18.3. 清除路由器日志记录

提问 清除路由器日志记录

回答

Router#**clear logging**

Clear logging buffer [confirm]**<enter>**

Router#

注释 无

18.4. 发送日志到屏幕显示

提问 在终端屏幕实时显示日志记录

回答

启用

Router#**terminal monitor**

Router#

禁用

Router#**terminal no monitor**

Router#

注释 缺省情况下日志记录只会在 console 端显示，要在 VTY 会话显示就必须使用上述命令

18.5. 使用远端日志服务器

提问 发送日志记录到远端日志服务器

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**logging *172.25.1.1***

Router(config)#**end**

Router#

12.2(15)T 后也可以使用下面命令格式

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**logging host *172.25.1.1***

Router2(config)#**end**

Router2#

注释 在 12.2(15)T 后增加了一个特性可以使发送的记录中包含了主机名，下面这是原始的日志记录

Jul 15 20:35:07 172.25.1.100: Jul 15 20:35:07.499 EDT: %SYS-5-CONFIG_I: Configured from console by ijbrown on vty0 (172.25.1.1)

下面这个是使用特性后的记录

Jul 15 20:37:05 172.25.1.100: **Router2:** Jul 15 20:37:05.173 EDT: %SYS-5-CONFIG_I: Configured from console by ijbrown on vty0 (172.25.1.1)

配置方法：Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**logging origin-id hostname**

Router2(config)#**end**

Router2#

18.6. UNIX 服务器上启用 SYSLOG 服务

提问 配置 Unix 服务器接收 syslog 记录

回答

一般只需要在*/etc/syslog.conf*

local7.info   /var/log/rtrlog

注释 缺省情况路由器使用 local7 logging facility

18.7. 修改缺省 LOG FACILITY

提问 修改缺省 Log Facility

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**logging host *172.25.1.1***

Router(config)#**logging facility *local6***

Router(config)#**end**

Router#

注释 无

18.8. 限制特定日志记录发送至服务器

提问 限制特定等级的日志记录发送至服务器

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**logging host *172.25.1.1***

Router(config)#**logging trap *notifications***

Router(config)#**end**

Router#

注释 无

18.9. 设定 SYSLOG 消息的源地址

提问 路由器 Syslog 消息的源地址使用特定地址

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**logging host *172.25.1.1***

Router(config)#**logging source-interface *Loopback0***

Router(config)#**end**

Router#

注释 这样如果在日志服务器上设置了地址翻译就可以实现下述的效果

Apr   2 20:27:01 172.25.2.6 94: %SYS-5-CONFIG_I: Configured from on vty0

Apr   2 20:27:48 Boston 95: %SYS-5-CONFIG_I: Configured from on vty0

18.10. 记录路由器日志记录到不同的文件

注释 略

18.11. 维护服务器上的日志记录

注释 使用脚本实现日志记录的自动存档等功能 略

18.12. 测试日志服务器的配置

注释 使用脚本来测试日志服务器的配置是否正确 略

18.13. 避免常见的消息被记录

提问 在日志记录中禁止一些常见的端口状态等消息

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**interface *Serial0/0***

Router(config-if)#**no logging event link-status**

Router(config-if)#**no logging event dlci-status-change**

Router(config-if)#**no logging event subif-link-status**

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 略

18.14. 日志记录的流量控制

提问 限制发送到服务器的日志流量

回答

```
Router#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router(config)#logging host 172.25.1.1
Router(config)#logging rate-limit 30 except warnings
Router(config)#end
Router#
```

对控制台口的日志记录数目控制

```
Router#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router(config)#logging rate-limit console 25 except warnings
Router(config)#end
Router#
```

注释 无

18.15. 启用日志统计

提问 统计路由器日志的类型和数目

回答

```
Router2#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router2(config)#logging count
Router2(config)#end
```

```
Router2#
```

注释

```
Router2#show logging count
Facility        Message Name                        Sev Occur       Last Time
==========================================================================================
NTP             PEERREACH                             6     3 Jul 13 20:31:34.441
NTP             PEERSYNC                              5     1 Jul 13 20:23:03.571
NTP             PEERUNREACH                           4     3 Jul 13 20:22:00.435
NTP             RESTART                               6     1 Jan 31 14:13:33.769
-------------  -------------------------------  ----------------------------------
NTP TOTAL                                                   8
```

18.16. 生成 XML 格式的日志记录

提问 以 XML 格式来发送日志

回答

```
Router2# configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router2(config)#logging console xml
Router2(config)#logging monitor xml
Router2(config)#logging buffered xml
Router2(config)#logging host 172.25.1.1 xml
Router2(config)#end
```

Router2#

注释 12.2(15)T 引入此特性，方便后处理

18.17. 修改日志记录

提问 希望修改系统日志记录的一些属性

回答

首先要写特定的 TCL 脚本（delcounters.tcl 脚本用于过滤掉包含 counters 的日志）

```
# delcounters.tcl    This script deletes all log messages that
#                              have the mnemonic "COUNTERS".
if { [string compare -nocase COUNTERS $::mnemonic ] == 0 } {
return ""
} else {
return $::orig_msg
}
```

然后引用此脚本

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**logging filter *tftp://172.25.1.1/delcounters.tcl***

Router2(config)#**logging host *172.25.1.1* filtered**

Router2(config)#**end**

Router2#

注释 Embedded Syslog Manager (ESM) 引自 12.3(2)T，提供一个程序化的接口可以对日志进行过滤，修改等全面控制，主要是使用 TCL 脚本来进行控制。

第十九章 访问列表

19.1. 基于源或者目的地址过滤

提问 阻止来自某地址或者发送至某地址的数据包

回答

使用标准控制列表来阻止特定源地址的数据包

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**access-list *50* deny host *10.2.2.2***

Router1(config)#**access-list *50* permit any**

Router1(config)#**interface *Serial0/1***

Router1(config-if)#**ip access-group *50* in**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

使用扩展控制列表来阻止特定源地址和目的地址的数据包

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**access-list *150* deny ip host *10.2.2.2* host *172.25.25.1***

Router1(config)#**access-list *150* permit ip any any**

Router1(config)#**interface *Serial0/1***

Router1(config-if)#**ip access-group *150* in**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 无

19.2. 给 ACL 添加注释

提问 给控制列表添加注释方便阅读

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**access-list *50* remark *Authorizing thy trespass with compare*** Router1(config)#**access-list *50* deny host *10.2.2.2***

Router1(config)#**access-list *50* permit *10.2.2.0 0.0.0.255***

Router1(config)#**access-list *50* permit any**

Router1(config)#**end**

Router1#

或者

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**ip access-list standard *TESTACL***

Router2(config-std-nacl)#**remark *Authorizing thy trespass with compare***

Router2(config-std-nacl)#**deny host *10.2.2.2***

Router2(config-std-nacl)#**permit *10.2.2.0 0.0.0.255***

Router2(config-std-nacl)#**permit any**

Router2(config-std-nacl)#**end**

Router2#

注释 在 show access list 命令中是看不到注释的

19.3. 基于应用过滤

提问 根据不同的应用来进行过滤

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**access-list *151* permit tcp any any eq www**

Router1(config)#**access-list *151* deny tcp any any gt *1023***

Router1(config)#**access-list *151* permit icmp any any**

Router1(config)#**access-list *151* permit udp any any eq ntp**

Router1(config)#**access-list *151* deny ip any any**

Router1(config)#**interface *Serial0/1***

Router1(config-if)#**ip access-group *151* in**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 无

19.4. 基于 TCP 头标签过滤

提问 根据 TCP 头字段中的标签位进行过滤

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**access-list *161* deny tcp any any ack fin psh rst syn urg**

Router1(config)#**access-list *161* deny tcp any any rst syn**

Router1(config)#**access-list *161* deny tcp any any rst syn fin**

Router1(config)#**access-list *161* deny tcp any any rst syn fin ack**

Router1(config)#**access-list *161* deny tcp any any syn fin**

Router1(config)#**access-list *161* deny tcp any any syn fin ack**

Router1(config)#**end**

Router1#

从 12.3(4)T 以后开始启用新的命令格式

Router2#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**ip access-list extended TCPFLAGFILTER**

Router2(config-ext-nacl)#**deny tcp any any match-all +ack +fin +psh +rst +syn +urg**

Router2(config-ext-nacl)#**deny tcp any any match-all +rst +syn**

Router2(config-ext-nacl)#**deny tcp any any match-all +rst +syn +fin**

Router2(config-ext-nacl)#**deny tcp any any match-all +rst +syn +fin +ack**

Router2(config-ext-nacl)#**deny tcp any any match-all +syn +fin**

Router2(config-ext-nacl)#**deny tcp any any match-all +syn +fin +ack**

Router2(config-ext-nacl)#**end**

Router2#

注释 TCP 头字段中有六种标签位设置 ACK，SYN，FIN，RST，PSH 和 URG。在新的命令格式中引入了 match-all 和 match-any 两个关键词，match-any 和传统过滤方式一致，只关心特定标志位设置而不管其他标志位设置，match-all 必须符合特定的标志位设置。

19.5. 限制 TCP 会话的方向

提问 过滤 TCP 会话 只允许客户端发起应用

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**access-list *148* permit tcp any eq telnet any established**

Router1(config)#**access-list *148* deny ip any any**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip access-group *148* in**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 无

19.6. 基于多端口应用的过滤

提问 过滤某些开启多端口的应用

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**access-list *152* permit tcp any any eq ftp**

Router1(config)#**access-list *152* permit tcp any any eq ftp-data established**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip access-group *152* in**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 对于其他多端口的可以使用下面的格式

Router1(config)#**access-list *154* permit udp any any range *6000 6063***

Router1(config)#**access-list *155* deny udp any any gt *1023***

Router1(config)#**access-list *156* permit udp any any lt *1024***

Router1(config)#**access-list *157* permit udp any any neq *666***

19.7. 基于 DSCP 和 TOS 的过滤

提问 根据 IP 服务质量信息进行过滤

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**access-list *162* permit ip any any dscp af11**

Router1(config)#**end**

或者

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**access-list *162* permit ip any any tos max-reliability**

Router1(config)#**end**

注释 无

19.8. 记录触发的控制列表

提问 记录触发控制列表的包信息

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**access-list *150* permit ip any any log**

Router1(config)#**interface *Serial0/1***

Router1(config-if)#**ip access-group *150* in**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

更详细点的信息

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**access-list *150* permit tcp any any log-input**

Router1(config)#**access-list *150* permit ip any any**

Router1(config)#**interface *Serial0/1***

Router1(config-if)#**ip access-group *150* in**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 第一个例子的日志信息

Feb 6 13:01:19: %SEC-6-IPACCESSLOGRP: list 150 permitted ospf 10.1.1.1 -> 224.0.0.5, 9 packets

Feb 6 13:01:19: %SEC-6-IPACCESSLOGDP: list 150 permitted icmp 10.1.1.1 -> 10.1.1.2 (0/0), 4 packets

第二个例子的日志信息

Feb 6 14:56:34: %SEC-6-IPACCESSLOGP: list 150 permitted tcp 172.25.1.1(0) (FastEthernet0/0.1 0010.4b09.5700) -> 172.25.25.1(0), 1 packet

注意的是 log-input 参数只能适应于扩展控制列表

19.9. 记录 TCP 会话

提问 记录 TCP 会话数目

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**access-list *122* permit tcp any any eq telnet established**

Router1(config)#**access-list *122* permit tcp any any eq telnet**

Router1(config)#**access-list *122* permit ip any any**

Router1(config)#**interface *Serial0/0***

Router1(config-if)#**ip access-group *122* in**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

或者

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**access-list *121* permit tcp any any eq telnet syn**

Router1(config)#**access-list *121* permit tcp any any eq telnet**

Router1(config)#**access-list *121* permit ip any any**

Router1(config)#**interface *Serial0/0***

Router1(config-if)#**ip access-group *121* in**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 对于第一个例子

Router1#**show access-list 122**

Extended IP access list 122

permit tcp any any eq telnet established (3843 matches)

permit tcp any any eq telnet (**6 matches**)

permit ip any any (31937 matches)

Router1#

从输出可以看到总共有六个 Telnet 会话通过接口，3,843 + 6 = 3,849 个 Telnet 数据包

19.10. 分析 ACL 日志条目

注释 使用脚本来分析生成的 ACL 日志，暂略

19.11. 使用命名和单反控制列表

提问 在命名控制列表中使用一个单反控制列表

回答

一个基本的命名控制列表类似数字控制列表

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip access-list standard *STANDARD-ACL***

Router1(config-std-nacl)#**remark *This is a standard ACL***

Router1(config-std-nacl)#**permit any log**

Router1(config-std-nacl)#**exit**

Router1(config)#**ip access-list extended *EXTENDED-ACL***

Router1(config-ext-nacl)#**remark *This is an extended ACL***

Router1(config-ext-nacl)#**deny tcp any any eq www**

Router1(config-ext-nacl)#**permit ip any any log**

Router1(config-ext-nacl)#**exit**

Router1(config)#**interface *Serial0/1***

Router1(config-if)#**ip access-group *STANDARD-ACL* in**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

下面是在其中内嵌单反控制列表来允许单反向的 Ping

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip access-list extended *PING-OUT***

Router1(config-ext-nacl)#**permit icmp any any reflect *ICMP-REFLECT* timeout *15***

Router1(config-ext-nacl)#**permit ip any any**

Router1(config-ext-nacl)#**exit**

Router1(config)#**ip access-list extended *PING-IN***

Router1(config-ext-nacl)#**evaluate *ICMP-REFLECT***

Router1(config-ext-nacl)#**deny icmp any any log**

Router1(config-ext-nacl)#**permit ip any any**

Router1(config-ext-nacl)#**exit**

Router1(config)#**interface *Serial0/1***

Router1(config-if)#**ip access-group *PING-OUT* out**

Router1(config-if)#**ip access-group *PING-IN* in**

Router1(config-if)#**end**

Router1#

注释 在例子中单反控制列表可以对返回的 ICMP Response 进行控制

19.12. 处理被动模式 FTP

提问 对被动模式的 FTP 来进行区分

回答

```
Router1#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router1(config)#access-list 144 permit tcp any gt 1023 any eq ftp
Router1(config)#access-list 144 permit tcp any gt 1023 any gt 1023
Router1(config)#access-list 144 deny ip any any
Router1(config)#interface Serial0/0.1
Router1(config-subif)#ip access-group 144 in
Router1(config-subif)#exit
Router1(config)#end
Router1#
```

注释 被动模式下的 FTP，客户端会再对服务器发送一个高于 1024 端口的链接，所以对于此类会话必须开启所有高于 1024 的端口，例子中的配置虽然能够解决此问题，但是减少了安全性，在以后的章节会介绍更有效的处理方式

19.13. 使用基于时间的控制列表

提问 对应用基于时间段进行控制

回答

```
Router1#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router1(config)#time-range NOSURF
Router1(config-time-range)# periodic weekdays 9:00 to 17:00
Router1(config-time-range)#exit
```

Router1(config)#**ip access-list extended *NOSURFING***

Router1(config-ext-nacl)# **deny tcp any any eq www time-range *NOSURF***

Router1(config-ext-nacl)# **permit ip any any**

Router1(config-ext-nacl)#**exit**

Router1(config)#**interface *FastEthernet0/1***

Router1(config-if)#**ip access-group *NOSURFING* in**

Router1(config-if)#**end**

Router1#

注释 在时间段的配置上你可以配置多个 periodic，

19.14. 基于非连续端口的过滤

提问 配置一种高效的非连续端口的过滤

回答

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**ip access-list extended *OREILLY***

Router2(config-ext-nacl)#**permit tcp any host *172.25.100.100* eq 80 23 25 110 514 21**

Router2(config-ext-nacl)#**end**

Router2#

注释 通常对于连续端口的过滤可以使用 **permit tcp any any range 20 25** 此类的命令，而对于非连续端口的过滤则要使用多个类似 **permit tcp any host *172.25.100.100* eq 80** 的命令，自从 12.3(7)T 以后则可以使用上例中的配置方式来进行简化。

19.15. 控制列表编辑

提问 直接对控制列表进行编辑

回答

插入一个条目至现有的控制列表中

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**ip access-list extended *OREILLY***

Router2(config-ext-nacl)#**12 permit tcp any host *172.25.100.100* eq 20**

Router2(config-ext-nacl)#**end**

Router2#

重新对控制列表序列号进行调整

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**ip access-list resequence OREILLY 10 10**

Router2(config)#**end**

Router2#

删除特定的控制列表条目

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**ip access-list extended *OREILLY***

Router2(config-ext-nacl)#**no *60***

Router2(config-ext-nacl)#**end**

Router2#

注释 从 12.3(2)T 以后路由器增加了对控制列表条目序列号的支持，缺省 10 递增，这样可以方便对控制列表进行编辑

Router2#**show ip access-lists *OREILLY***

Extended IP access list OREILLY

10 permit tcp any host 172.25.100.100 eq www

20 permit tcp any host 172.25.100.100 eq telnet

30 permit tcp any host 172.25.100.100 eq smtp

40 permit tcp any host 172.25.100.100 eq pop3

50 permit tcp any host 172.25.100.100 eq cmd

19.16. 基于 IPV6 过滤

提问 对 Ipv6 的数据包进行过滤

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ipv6 access-list *EXAMPLES***

Router1(config-ipv6-acl)#**permit ipv6 *AAAA:5::/64* any**

Router1(config-ipv6-acl)#**permit ipv6 host *AAAA:5::FE:1* any**

Router1(config-ipv6-acl)#**permit tcp any any eq telnet established**

Router1(config-ipv6-acl)#**deny tcp any any eq telnet syn**

Router1(config-ipv6-acl)#**sequence *55* permit udp any any eq snmp**

Router1(config-ipv6-acl)#**remark *this is a comment***

Router1(config-ipv6-acl)#**sequence *66* remark *this comment has a sequence number***

```
Router1(config-ipv6-acl)#permit icmp any any reflect ICMP-REFLECT
Router1(config-ipv6-acl)#deny ipv6 any host AAAA:6::1 log
Router1(config-ipv6-acl)#deny ipv6 any any log-input
Router1(config-ipv6-acl)#exit
Router1(config)#interface FastEthernet0/0
Router1(config-if)#ipv6 traffic-filter EXAMPLES in
Router1(config-if)#exit
Router1(config)#end
Router1#
```

注释 Ipv6 过滤只能使用命名式控制列表，当然也继承了命名式控制列表的所有优点。

第二十章 DHCP

20.1. 使用 IP HELPER ADDRESSES 命令

提问 配置路由器对 DHCP Request 转发的支持

回答

```
Router1#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router1(config)#interface Ethernet0
Router1(config-if)#ip helper-address 172.25.1.1
Router1(config-if)#ip helper-address 172.25.10.7
Router1(config-if)#exit
Router1(config)#end
```

Router1#

注释 使用 IP Helper Address 命令把路由器配置成为一个 DHCP 代理服务器，转发客户端的 DHCP Request 至配置的 ip helper address。

20.2. 限制 IP HELPER ADDRESSES 命令的影响

提问 配置 IP Helper Address 命令以后导致链路利用率增高或者 DHCP 服务器负荷增高

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**no ip forward-protocol udp tftp**

Router1(config)#**no ip forward-protocol udp nameserver**

Router1(config)#**no ip forward-protocol udp domain**

Router1(config)#**no ip forward-protocol udp time**

Router1(config)#**no ip forward-protocol udp netbios-ns**

Router1(config)#**no ip forward-protocol udp netbios-dgm**

Router1(config)#**no ip forward-protocol udp tacacs**

Router1(config)#**end**

Router1#

注释 缺省情况下 IP Helper 命令会转发很多 UDP 广播数据包，不仅仅是 DHCP 数据包，并且不能针对不同的服务器转发不同的广播包

20.3. 使用 DHCP 来动态配置路由器 IP 地址

提问 配置路由器动态获得 IP 地址

回答

```
Router1#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router1(config)#interface FastEthernet0/1
Router1(config-if)#ip address dhcp
Router1(config-if)#end
Router1#
Interface FastEthernet0/1 assigned DHCP address 172.25.1.57, mask 255.255.255.0
Router1#
```

注释 在 12.2(8)T 之前此命令仅仅适用于以太网接口。从 12.3(8)T 以后可以对 DHCP 选项进行控制，下例配置为不获得 DNS 服务器

```
Router1#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router1(config)#interface FastEthernet0/1
Router1(config-if)#no ip dhcp client request dns-nameserver
Router1(config-if)#end
```

另外对于获得的缺省路由，管理距离为 254

```
S*     0.0.0.0/0 [254/0] via 172.25.1.1
```

从 12.3(4)T 开始增加了对获得地址释放和重新获得的支持

```
Router1#release dhcp FastEthernet0/1
Router1#renew dhcp FastEthernet0/1
```

20.4. 通过 DHCP 来对客户端进行动态 IP 地址分配

提问 配置路由器成为 DHCP 服务器

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**service dhcp**

Router1(config)#**ip dhcp pool *172.25.1.0/24***

Router1(dhcp-config)#**network *172.25.1.0 255.255.255.0***

Router1(dhcp-config)#**default-router *172.25.1.1***

Router1(dhcp-config)#**exit**

Router1(config)#**ip dhcp excluded-address *172.25.1.1 172.25.1.50***

Router1(config)#**ip dhcp excluded-address *172.25.1.200 172.25.1.255***

Router1(config)#**end**

Router1#

注释 注意的是要配置 excluded 命令来排除某些地址，防止出现地址冲突

20.5. 配置 DHCP 的配置选项

提问 配置更多的 DHCP 配置选项提供给客户端

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip dhcp pool *ORAserver***

Router1(dhcp-config)#**host *172.25.1.34 255.255.255.0***

Router1(dhcp-config)#**client-name *bigserver***

Router1(dhcp-config)#**default-router *172.25.1.1 172.25.1.3***

Router1(dhcp-config)#**domain-name *oreilly.com***

Router1(dhcp-config)#**dns-server *172.25.1.1 10.1.2.3***

Router1(dhcp-config)#**netbios-name-server *172.25.1.1***

Router1(dhcp-config)#**netbios-node-type *h-node***

Router1(dhcp-config)#**option 66 ip *10.1.1.1***

Router1(dhcp-config)#**option 33 ip *192.0.2.1 172.25.1.3***

Router1(dhcp-config)#**option 31 hex 01**

Router1(dhcp-config)#**lease 2**

Router1(dhcp-config)#**exit**

Router1(config)#**end**

Router1#

注释 Option 66 定义 TFTP 服务器; Option 33 定义静态路由; Option 31 定义客户端使用 IRDP.

20.6. 配置 DHCP 的分配时长

提问 修改缺省 DHCP 分配时长

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip dhcp pool *172.25.2.0/24***

Router1(dhcp-config)#**lease 2 12 30**

Router1(dhcp-config)#**exit**

Router1(config)#**end**

Router1#

注释 缺省分配为一天，配置选项为天，小时，分钟

20.7. 分配静态 IP 地址

提问 每次都分配给某个特定设备特定 IP 地址

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip dhcp pool *IAN***

Router1(dhcp-config)#**host *172.25.1.33 255.255.255.0***

Router1(dhcp-config)#**client-identifier *0100.0103.85e9.87***

Router1(dhcp-config)#**client-name *win2k***

Router1(dhcp-config)#**default-router *172.25.1.1***

Router1(dhcp-config)#**domain-name *oreilly.com***

Router1(dhcp-config)#**dns-server *172.25.1.1***

Router1(dhcp-config)#**exit**

Router1(config)#**end**

Router1#

注释 这里通过 MAC 地址来绑定某个 IP 地址。Client-identifier 后面跟的是 MAC 地址，不过比传统 MAC 地址多了 0100，代表是以太网，对于更多的媒介类型值参考 RFC 3232 中的 Number Hardware Type 部分

Router1#**show ip dhcp binding**

IP address	Hardware address	Lease expiration	Type
172.25.1.33	0100.0103.85e9.87	Infinite	Manual
172.25.1.52	0100.50da.2a5e.a2	Apr 11 2006 09:00 PM	Automatic
172.25.1.53	0100.0103.ea1b.ed	Apr 11 2006 08:58 PM	Automatic

20.8. 配置一个 DHCP 数据库客户端

提问 在另一个设备上备份当前的 DHCP 数据库

回答

FTP 方式

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip dhcp database** ***ftp://dhcp:bindsave@172.25.1.1/dhcp-leases***

Router1(config)#**end**

Router1#

TFTP 方式

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip dhcp database** ***tftp://172.25.1.1/dhcp-leases***

Router1(config)#**end**

Router1#

RCP 方式

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip dhcp database** ***rcp://dhcp@172.25.1.1/dhcp-leases***

Router1(config)#**end**

Router1#

注释 通常 DHCP 数据库保存于内存，如果重启就会丢失，可以使用上述方式进行备份从而不会丢失，通过下述命令验证

Router1#**show ip dhcp database**

URL   : ftp://dhcp:bindsave@172.25.1.1/dhcp-leases

Read   : Never

Written   : Apr 09 2006 10:24 PM

Status   : Last write succeeded. Agent information is up-to-date.

Delay   : 300 seconds

Timeout   : 300 seconds

Failures : 1

Successes: 30

20.9. 在同一子网配置多个 DHCP 服务器

提问 在同一子网配置多个 DHCP 服务器来增加可用性

回答

Router1:

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip dhcp pool** ***172.22.1.0/24***

Router1(dhcp-config)#**network** ***172.22.1.0 255.255.255.0***

Router1(dhcp-config)#**default-router** ***172.22.1.1***

Router1(dhcp-config)#**domain-name** ***oreilly.com***

Router1(dhcp-config)#**dns-server** ***172.25.1.1 10.1.2.3***

Router1(dhcp-config)#**exit**

Router1(config)#**ip dhcp excluded-address** ***172.22.1.1 172.22.1.49***

Router1(config)#**ip dhcp excluded-address** ***172.22.1.150 172.22.1.254***

Router1(config)#**ip dhcp database** ***ftp://dhcp:bindsave@172.25.1.1/dhcp-leases-rtr1***

Router1(config)#**end**

Router1#

Router2:

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**ip dhcp pool** ***172.22.1.0/24***

Router2(dhcp-config)#**network** ***172.22.1.0 255.255.255.0***

Router2(dhcp-config)#**default-router** ***172.22.1.1***

Router2(dhcp-config)#**domain-name** ***oreilly.com***

Router2(dhcp-config)#**dns-server** ***172.25.1.1 10.1.2.3***

Router2(dhcp-config)#**exit**

Router2(config)#**ip dhcp excluded-address** ***172.22.1.1 172.22.1.149***

Router2(config)#**ip dhcp database** ***ftp://dhcp:bindsave@172.25.1.1/dhcp-leases-rtr2***

Router2(config)#**end**

Router2#

注释 要确保配置的地址池不重复，Router1 分配地址为从 172.25.1.50 到 172.25.1.149, Router2 分配地址为从 172.25.1.150 到 172.25.1.254,

20.10. DHCP 静态映射

提问 根据某个文本文件来进行 IP 地址的静态指配

回答

先在 TFTP 服务器上创建此文本文件

Freebsd% **cat *`/tftpboot/dhcp.static`***

```
*time* Aug 17 2006 03:52 PM

*version* 2

!IP address      Type     Hardware address          Lease expiration

10.1.1.16 /24    id       0100.104b.33da.74         Infinite

10.1.1.17 /24    id       0100.0dbc.eff6.38         Infinite

10.1.1.18 /24    id       0100.0a5e.4001.27         Infinite

10.1.1.19 /24    id       0100.0331.327e.41         Infinite

10.1.1.20 /24    id       0100.0d60.b21a.4c         Infinite

*end*

Freebsd%
```

路由器配置

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip dhcp pool *OREILLY***

Router1(dhcp-config)#**origin file *tftp://172.25.1.1/dhcp.static***

Router1(dhcp-config)#**default-router *10.1.1.1***

Router1(dhcp-config)#**dns-server *172.25.1.1 172.25.1.3***

Router1(dhcp-config)#**domain-name *oreilly.com***

Router1(dhcp-config)#**lease *3***

Router1(dhcp-config)#**end**

Router1#

注释 20.7 讲到的静态地址分配需要一个特定的 DHCP Pool，扩展性不强，从 12.3(11)T 以后可以使用特定的文本文件来进行指配，不过必须遵照一定的格式。如果文本文件修改后需要生效，必须先 **no service dhcp** 来停止 DHCP 服务然后 **service dhcp** 命令重新启用来生效

20.11. 安全 DHCP IP 地址指派

提问 同步 ARP 和 DHCP 地址绑定来防止出现 IP 地址欺骗

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip dhcp pool *OREILLY***

Router1(dhcp-config)#**update arp**

Router1(dhcp-config)#**end**

Router1#

注释 从 12.2(15)T 开始思科引入了安全 DHCP IP 地址指派（DHCP secured IP address assignment），启用此特性后会针对每个 DHCP 绑定增加一个安全 ARP 条目，从而防止对此条目的修改，即使使用 clear arp-cache 命令也会保证此条目不被清除

20.12. 显示 DHCP 状态

提问 显示 DHCP 服务器的状态

回答

显示绑定和相应的分配时长

Router1#**show ip dhcp binding**

显示地址冲突

Router1#**show ip dhcp conflict**

显示数据库状态

Router1#**show ip dhcp database**

显示全局 DHCP 数据统计

Router1#**show ip dhcp server statistics**

注释

Router1#**show ip dhcp server statistics**

Memory usage 17996

Address pools 4

Database agents 1

Automatic bindings 2

Manual bindings 1

Expired bindings 3

Malformed messages 0

Message Received

BOOTREQUEST 0

DHCPDISCOVER 63

DHCPREQUEST 203

DHCPDECLINE 1

DHCPRELEASE 27

DHCPINFORM 19

Message Sent

BOOTREPLY 0

DHCPOFFER 63

DHCPACK 139

DHCPNAK 2

Router1#

20.13. DHCP 排错

提问 对 DHCP 出现的问题进行排错

回答

Router1#**debug ip dhcp server events**

Router1#**debug ip dhcp server packet**

注释 无

第二十一章 NAT

21.1. 配置基本 NAT 功能

提问 在路由器上启用基本的 NAT 功能

回答

```
Router#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router(config)#access-list 15 permit 192.168.0.0 0.0.255.255
Router(config)#ip nat inside source list 15 interface FastEthernet0/0 overload
Router(config)#interface FastEthernet0/2
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface Ethernet0/0
Router(config-if)#ip address 172.16.1.5 255.255.255.252
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#end
Router#
```

注释 例子中的配置实现了对地址段 192.168.0.0/16 访问外部网络重写为 172.16.1.5 的功能，基本的地址翻译功能

21.2. 动态转化为外部地址

提问 从某个特定的地址池来动态分配地址

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**access-list *15* permit *192.168.0.0 0.0.255.255***

Router(config)#**ip nat pool *NATPOOL 172.16.1.100 172.16.1.150* netmask *255.255.255.0***

Router(config)#**ip nat inside source list *15* pool *NATPOOL***

Router(config)#**interface *FastEthernet 0/0***

Router(config-if)#**ip address *192.168.1.1 255.255.255.0***

Router(config-if)#**ip nat inside**

Router(config-if)#**exit**

Router(config)#**interface *FastEthernet 0/1***

Router(config-if)#**ip address *192.168.2.1 255.255.255.0***

Router(config-if)#**ip nat inside**

Router(config-if)#**exit**

Router(config)#**interface *Ethernet1/0***

Router(config-if)#**ip address *172.16.1.2 255.255.255.0***

Router(config-if)#**ip nat outside**

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 **ip nat inside source list *15* pool *NATPOOL*** 定义了翻译出去的地址池，如果地址池用完新的翻译将不成功，如果加上了 overload 参数将会从第一个地址开始进行复用。另外这里的地址池并不一定要和 outside 端口的地址在同一网段，只要有相应的路由就可以

21.3. 静态转化为外部地址

提问 翻译某些特定的内部地址为特定的外部地址

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**ip nat inside source static *192.168.1.15 172.16.1.10***

Router(config)#**ip nat inside source static *192.168.1.16 172.16.1.11***

Router(config)#**interface *FastEthernet 0/0***

Router(config-if)#**ip address *192.168.1.1 255.255.255.0***

Router(config-if)#**ip nat inside**

Router(config-if)#**exit**

Router(config)#**interface *FastEthernet 0/1***

Router(config-if)#**ip address *192.168.2.1 255.255.255.0***

Router(config-if)#**ip nat inside**

Router(config-if)#**exit**

Router(config)#**interface *Ethernet1/0***

Router(config-if)#**ip address *172.16.1.2 255.255.255.0***

Router(config-if)#**ip nat outside**

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 静态地址翻译

21.4. 地址静态和动态翻译结合

提问 静态和动态地址翻译相结合

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**access-list *15* deny *192.168.1.15 0.0.0.0***

Router(config)#**access-list *15* deny *192.168.1.16 0.0.0.0***

Router(config)#**access-list *15* permit *192.168.0.0 0.0.255.255***

Router(config)#**ip nat inside source static *192.168.1.15 172.16.1.10***

Router(config)#**ip nat inside source static *192.168.1.16 172.16.1.11***

Router(config)#**ip nat pool *NATPOOL 172.16.1.100 172.16.1.150* netmask *255.255.255.0***

Router(config)#**ip nat inside source list *15* pool *NATPOOL* overload**

Router(config)#**interface *FastEthernet0/0***

Router(config-if)#**ip address *192.168.1.1 255.255.255.0***

Router(config-if)#**ip nat inside**

Router(config-if)#**exit**

Router(config)#**interface *FastEthernet0/1***

Router(config-if)#**ip address *192.168.2.1 255.255.255.0***

Router(config-if)#**ip nat inside**

Router(config-if)#**exit**

Router(config)#**interface *Ethernet0/0***

Router(config-if)#**ip address *172.16.1.2 255.255.255.0***

Router(config-if)#**ip nat outside**

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 这里的控制列表把所要静态内部地址排除了，当然这一步也不是必须的，因为静态翻译的优先级要高于动态翻译的，不过静态翻译的外部地址必须要从动态翻译的地址池中排除。

21.5. 使用 ROUTE MAPS 来进行翻译规则控制

提问 使用 Route Maps 来进行更好的静态地址翻译

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**interface *FastEthernet0/0***

Router(config-if)#**ip address *172.16.1.5 255.255.255.252***

Router(config-if)#**ip nat outside**

Router(config-if)#**exit**

Router(config)#**interface *FastEthernet0/1***

Router(config-if)#**ip address *172.16.2.5 255.255.255.252***

Router(config-if)#**ip nat outside**

Router(config-if)#**exit**

Router(config)#**interface *FastEthernet0/2***

Router(config-if)#**ip address *192.168.1.1 255.255.255.0***

Router(config-if)#**ip nat inside**

Router(config-if)#**exit**

Router(config)#**ip nat inside source route-map *ISP-1* interface *FastEthernet0/0* overload**

Router(config)#**ip nat inside source route-map *ISP-2* interface *FastEthernet0/1* overload**

Router(config)#**route-map *ISP-1* permit *10***

Router(config-route-map)#**match interface *FastEthernet0/0***

Router(config-route-map)#**exit**

Router(config)#**route-map *ISP-2* permit *10***

Router(config-route-map)#**match interface *FastEthernet0/1***

Router(config-route-map)#**exit**

Router(config)#**end**

Router#

注释 适用于多个 outside 端口的情况

21.6. 同时两个方向地址翻译

提问 同时对内部地址和外部地址进行翻译

回答

Router#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**access-list** ***15*** **deny** ***192.168.1.15***

Router(config)#**access-list** ***15*** **permit** ***192.168.0.0 0.0.255.255***

Router(config)#**access-list** ***16*** **deny** ***172.16.5.25***

Router(config)#**access-list** ***16*** **permit** ***172.16.0.0 0.0.255.255***

Router(config)#**ip nat pool** ***NATPOOL 172.16.1.100 172.16.1.150*** **netmask** ***255.255.255.0***

Router(config)#**ip nat pool** ***INBOUNDNAT 192.168.15.100 192.168.15.200*** **netmask** ***255.255.255.0***

Router(config)#**ip nat inside source list** ***15*** **pool** ***NATPOOL*** **overload**

Router(config)#**ip nat inside source list** ***16*** **pool** ***INBOUNDNAT*** **overload**

Router(config)#**ip nat inside source static** ***192.168.1.15 172.16.1.10***

Router(config)#**ip nat outside source static** ***172.16.5.25 192.168.15.5***

Router(config)#**ip route** ***192.168.15.0 255.255.255.0*** **Ethernet*0/0***

Router(config)#**interface** ***FastEthernet 0/0***

Router(config-if)#**ip address** ***192.168.1.1 255.255.255.0***

Router(config-if)#**ip nat inside**

Router(config-if)#**exit**

Router(config)#**interface** ***FastEthernet 0/1***

Router(config-if)#**ip address** ***192.168.2.1 255.255.255.0***

Router(config-if)#**ip nat inside**

Router(config-if)#**interface** ***Ethernet0/0***

Router(config-if)#**ip address** ***172.16.1.2 255.255.255.0***

Router(config-if)#**ip nat outside**

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 暂无

21.7. 网络前缀重写

提问 简单的改变某个网络段的前缀

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**ip nat outside source static network *172.16.0.0 172.17.0.0 /16* no-alias**

Router(config)#**ip route *172.16.0.0 255.255.0.0* Ethernet*1/0***

Router(config)#**ip route *172.17.0.0 255.255.0.0* Ethernet*1/0***

Router(config)#**interface *FastEthernet 0/0***

Router(config-if)#**ip address *10.1.1.1 255.255.255.0***

Router(config-if)#**ip nat inside**

Router(config-if)#**exit**

Router(config)#**interface *Ethernet1/0***

Router(config-if)#**ip address *172.16.1.6 255.255.255.252***

Router(config-if)#**ip nat outside**

Router(config-if)#**exit**

Router(config)#**end**

Router#

注释 适用于两个网络互访而地址段冲突的情况

21.8. 使用 NAT 来进行服务器负荷分担

提问 多个服务器使用同一 IP 地址从而实现应用的负荷分担

回答

```
Router#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router(config)#interface FastEthernet0/0
Router(config-if)#ip address 192.168.1.1 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip nat pool WEBSERVERS 192.168.1.101 192.168.1.105 netmask 255.255.255.0 type rotary
Router(config)#access-list 20 permit host 192.168.1.100
Router(config)#ip nat inside destination list 20 pool WEBSERVERS
Router(config)#end
Router#
```

注释 这里不同点在于使用了 rotary 的参数和使用了 destination 而不是 source 在翻译规则中，当然这种是穷人的负载均衡解决方案

21.9. 基于状态的 NAT 切换

提问 在高可用性网络中部署 NAT，这样一台设备坏掉的情况下另一台可以切换起到 NAT 作用

回答

RouterA

Router-A#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router-A(config)#**access-list *11* permit any**

Router-A(config)#**ip nat pool *NATPOOL 172.17.100.100 172.17.100.150* netmask *255.255.255.0***

Router-A(config)#**ip nat inside source list *11* pool *NATPOOL* mapping-id *1***

Router-A(config)#**interface *FastEthernet0/0***

Router-A(config-if)#**ip address *192.168.1.3 255.255.255.0***

Router-A(config-if)#**ip nat inside**

Router-A(config-if)#**standby *1* ip *192.168.1.1***

Router-A(config-if)#**standby *1* preempt**

Router-A(config-if)#**standby *1* name *SNATGROUP***

Router-A(config-if)#**exit**

Router-A(config)#**interface *Serial0/0***

Router-A(config-if)#**ip address *172.17.55.2 255.255.255.252***

Router-A(config-if)#**ip nat outside**

Router-A(config-if)#**exit**

Router-A(config)#**ip nat Stateful id *1***

Router-A(config-ipnat-snat)#**redundancy *SNATGROUP***

Router(config-ipnat-snat-red)#**mapping-id** ***1***

Router(config-ipnat-snat-red)#**exit**

Router-A(config)#**end**

Router-A#

RouterB

Router-B#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-B(config)#**access-list** ***11*** **permit any**

Router-B(config)#**ip nat pool** ***NATPOOL 172.17.100.100 172.17.100.150*** **netmask** ***255.255.255.0***

Router-B(config)#**ip nat inside source list** ***11*** **pool** ***NATPOOL*** **mapping-id** ***1***

Router-B(config)#**interface** ***FastEthernet0/0***

Router-B(config-if)#**ip address** ***192.168.1.2 255.255.255.0***

Router-B(config-if)#**ip nat inside**

Router-B(config-if)#**standby** ***1*** **ip** ***192.168.1.1***

Router-B(config-if)#**standby** ***1*** **priority** ***90***

Router-B(config-if)#**standby** ***1*** **preempt**

Router-B(config-if)#**standby** ***1*** **name** ***SNATGROUP***

Router-B(config-if)#**exit**

Router-B(config)#**interface** ***Serial0/0***

Router-B(config-if)#**ip address** ***172.17.55.6 255.255.255.252***

Router-B(config-if)#**ip nat outside**

Router-B(config-if)#**exit**

Router-B(config)#**ip nat Stateful id *1***

Router-B(config-ipnat-snat)#**redundancy *SNATGROUP***

Router(config-ipnat-snat-red)#**mapping-id *1***

Router(config-ipnat-snat-red)#**exit**

Router-B(config)#**end**

Router-B#

注释 虽然说通过使用 HSRP 可以解决可用性的问题，但是不能同步 NAT 翻译表，从 12.2(13)T 以后思科引入了基于状态的 NAT（SNAT），这样可以保持两台设备的翻译表同步，其关键命令为 *ip nat Stateful* 要注意的是这里的 Stateful 是大写开头的，这里是区分大小写的。另外 SNAT 只和 HSRP 连用，不能跟 VRRP 或者 GLBP 一起作用。同时也可以使用多组 HSRP 的形式来保持负载均衡。

21.10. 调整 NAT 时长

提问 调整 NAT 翻译表中条目的时长

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**ip nat translation tcp-timeout *500***

Router(config)#**ip nat translation udp-timeout *30***

Router(config)#**ip nat translation dns-timeout *30***

Router(config)#**ip nat translation icmp-timeout *30***

Router(config)#**ip nat translation finrst-timeout *30***

Router(config)#**ip nat translation syn-timeout *30***

Router(config)#**end**

Router#

也可以限制翻译表的最大条目数

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**ip nat translation max-entries *1000***

Router(config)#**end**

Router#

注释 缺省 TCP 为 24 小时，UDP 为 5 分钟，DNS 为 1 分钟

21.11. 修改 FTP 的 TCP 端口

提问 FTP 服务器使用非正常端口

回答

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**access-list *19* permit *192.168.55.5***

Router(config)#**ip nat service list *19* ftp tcp port *8021***

Router(config)#**ip nat service list *19* ftp tcp port *21***

Router(config)#**end**

Router#

注释 在 12.2(4)T 后思科引入了 no-payload 关键词来防止对数据包载荷的地址信息进行修改

Router#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router(config)#**interface *FastEthernet0/0***

Router(config-if)#**ip address *172.16.1.5 255.255.255.252***

Router(config-if)#**ip nat outside**

Router(config-if)#**exit**

Router(config)#**interface *FastEthernet0/1***

Router(config-if)#**ip address *192.168.1.1 255.255.255.0***

Router(config-if)#**ip nat inside**

Router(config-if)#**exit**

Router(config)#**ip nat inside source static *192.168.1.10 172.16.1.5* no-payload**

Router(config)#**end**

Router#

21.12. 检查 NAT 状态

提问 查看当前 NAT 信息

回答

Router#**show ip nat translation**

Router#**clear ip nat translation ***

Router#**clear ip nat translation inside *172.18.3.2***

Router#**clear ip nat translation outside *192.168.1.10***

Router#**show ip nat statistics**

Router#**clear ip nat statistics**

注释 Router#**show ip nat translation**

Pro Inside global Inside local Outside local Outside global

"Inside global" 为内部设备翻译的地址"Inside local"为内部设备的真实地址"Outside local" 为外部设备翻译的地址"Outside global" 为外部设备的真实地址，global addresses 在 outside, local addresses 在 inside.

21.13. NAT 排错

提问 对 NAT 进行排错

回答

Router#**debug ip nat**

Router#**debug ip nat detailed**

Router#**debug ip nat *15***

Router#**debug ip nat *15* detailed**

注释 无

第二十二章 第一跳冗余协议

22.1. 配置基本 HSRP

提问 当主用路由器当掉以后备份路由器可以接管主用路由器的 IP 地址和 MAC 地址

回答

Router1：

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *FastEthernet 0/1***

Router1(config-if)#**ip address *172.22.1.3 255.255.255.0***

Router1(config-if)#**standby 1 ip *172.22.1.1***

Router1(config-if)#**standby 1 priority *120***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

Router2：

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**interface *FastEthernet 1/0***

Router2(config-if)#**ip address *172.22.1.2 255.255.255.0***

Router2(config-if)#**standby 1 ip *172.22.1.1***

Router2(config-if)#**standby 1 priority *110***

Router2(config-if)#**exit**

Router2(config)#**end**

Router2#

注释 由于 HSRP 虚拟出来的 MAC 地址跟组相关，所以可能会出现同一交换机收到多个相同的 MAC 地址的情况，这时候就需要用 **standby *1* mac-address *0000.0c07.ad01*** 命令来人工指定一个 MAC 地址

22.2 使用 HSRP 强占特性

提问 强制某个路由器启动后一直在组中处于主用状态

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface *FastEthernet 0/1***

Router1(config-if)#**standby 1 ip *172.22.1.1***

Router1(config-if)#**standby 1 priority *120***

Router1(config-if)#**standby 1 preempt**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**interface *FastEthernet 1/0***

Router2(config-if)#**standby 1 ip *172.22.1.1***

Router2(config-if)#**standby 1 priority *110***

Router2(config-if)#**standby 1 preempt**

Router2(config-if)#**exit**

Router2(config)#**end**

Router2#

注释 正常情况下当 LAN 端口 up 后就会发生强占，而此时可能网络还没有收敛，所以建议配置强占延迟时间，让路由器启动后过一段时间再发起强占 standby 1 preempt delay 60

22.3. 配置 HSRP 对接口问题追踪的支持

提问 当主用路由器的上联端口出现问题后主动切换到备用路由器

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface *FastEthernet0/1***

Router1(config-if)#**standby 1 ip *172.22.1.1***

Router1(config-if)#**standby 1 priority *120***

Router1(config-if)#**standby 1 preempt**

Router1(config-if)#**standby 1 track *Serial0/0 20***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

从 12.2(15)T 后引入更多可追踪实例

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**track *11* interface *Serial1/1* ip routing**

Router1(config-track)#**exit**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**standby *1* ip *172.22.1.1***

Router1(config-if)#**standby *1* priority *120***

Router1(config-if)#**standby *1* preempt**

Router1(config-if)#**standby *1* track *11* decrement *50***

Router1(config-if)#**end**

Router1#

注释 Router1#**show track**

Track 11

  Interface Serial1/1 ip routing

IP routing is Down (hw admin-down, ip disabled)

1 change, last change 00:12:48

Tracked by:

HSRP FastEthernet0/0 1

22.4. HSRP 负载均衡

提问 在两台或者多台 HSRP 路由器上实现流量的负载均衡

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *FastEthernet0/1***

Router1(config-if)#**ip address *172.22.1.3 255.255.255.0***

Router1(config-if)#**standby 1 ip *172.22.1.1***

Router1(config-if)#**standby 1 priority 120**

Router1(config-if)#**standby 1 preempt**

Router1(config-if)#**standby 2 ip *172.22.1.2***

Router1(config-if)#**standby 2 priority 110**

Router1(config-if)#**standby 2 preempt**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**interface *FastEthernet1/0***

Router2(config-if)#**ip address *172.22.1.4 255.255.255.0***

Router2(config-if)#**standby 1 ip *172.22.1.1***

Router2(config-if)#**standby 1 priority 110**

Router2(config-if)#**standby 1 preempt**

Router2(config-if)#**standby 2 ip *172.22.1.2***

Router2(config-if)#**standby 2 priority 120**

Router2(config-if)#**standby 2 preempt**

Router2(config-if)#**exit**

Router2(config)#**end**

Router2#

注释 由于出现两个网关，所以需要在终端设备上分开配置各自的缺省网关。

22.5.   HSRP 中 ICMP 重定向

提问 在 HSRP 中启用 ICMP 重定向

回答

Router2#configure terminal

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#interface FastEthernet 1/0

Router2(config-if)#no ip redirects

Router2(config-if)#standby redirects disable

Router2(config-if)#exit

Router2(config)#end

Router2#

注释 无

22.6. 调整 HSRP 定时器

提问 调整备份路由器接管主用路由器所需时长

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *FastEthernet0/1***

Router1(config-if)#**standby 1 ip *172.22.1.1***

Router1(config-if)#**standby 1 priority *120***

Router1(config-if)#**standby 1 preempt**

Router1(config-if)#**standby 1 timers *1 3***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 缺省 Hello 包时长为 3 秒，10 秒后会接管，如果主用路由器调整时长，整个组内的路由器都要调整为相同的时长。最短可以到达毫秒 Router1(config-if)#standby 1 timers msec 100 msec 300

22.7. 在令牌环网络中使用 HSRP

提问 在令牌环网络中配置 HSRP

回答

如果只用 IP 协议配置同前面例子，如果还有其他协议，特别是使用了 source-route bridging 就用下面的配置方法

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface *Tokenring0***

Router1(config-if)#**ip address *172.22.1.3***

Router1(config-if)#**standby ip *172.22.1.1***

Router1(config-if)#**standby use-bia**

Router1(config-if)#**standby priority *120***

Router1(config-if)#**standby preempt**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**interface *Tokenring0***

Router2(config-if)#**ip address *172.22.1.2***

Router2(config-if)#**standby ip *172.22.1.1***

Router2(config-if)#**standby use-bia**

Router2(config-if)#**standby priority *110***

Router2(config-if)#**standby preempt**

Router2(config-if)#**exit**

Router2(config)#**end**

Router2#

注释 由于令牌环网络会用到设备的 MAC 地址信息，所以如果 HSRP 用到虚拟 MAC 就会出问题，因此在配置中使用了 burned-in address (BIA)来代替 MAC 来避免出现问题

22.8. 配置 HSRP 的 SNMP 支持

提问 启用 HSRP 的 SNMP Traps

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**snmp-server enable traps hsrp**

Router1(config)#**snmp-server host *172.25.1.1 ORATRAP***

Router1(config)#**end**

Router1#

注释 无

22.9. 增加 HSRP 的安全性

提问 提高 HSRP 的安全

回答

组内设备使用相同的配置

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *FastEthernet 0/1***

Router1(config-if)#**standby 1 ip *172.22.1.1***

Router1(config-if)#**standby 1 priority *120***

Router1(config-if)#**standby 1 authentication *NEOSHI***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

从 12.3(2)T 后支持 MD5 加密密码

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface *FastEthernet0/1***

Router1(config-if)#**standby *1* ip *10.1.1.1***

Router1(config-if)#**standby *1* priority *200***

Router1(config-if)#**standby *1* authentication md5 key-string *OREILLY***

Router1(config-if)#**end**

Router1#

为了防止其他路由器成为主用路由器，设置本路由器高优先级

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface *FastEthernet 0/1***

Router1(config-if)#**standby 1 ip *172.22.1.1***

Router1(config-if)#**standby 1 priority *255***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 无

22.10. 显示 HSRP 状态信息

提问 显示 HSRP 状态信息

回答

Router2#**show standby**

Router2#**show standby *FastEthernet 1/0***

Router2#**show standby brief**

注释 无

22.11. HSRP 排错

提问 对 HSRP 进行排错

回答

Router2#**debug standby errors**

Router2#**debug standby events**

Router2#**debug standby packets**

Router2#**debug standby terse**

注释 无

22.12. 启用 HSRP 版本 2

提问 部署 HSRPv2

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**interface *FastEthernet0/1***

Router1(config-if)#**standby version 2**

Router1(config-if)#**standby *4095* ip *10.1.1.1***

Router1(config-if)#**standby *4095* timers msec *15* msec *50***

Router1(config-if)#**standby *4095* priority *200***

Router1(config-if)#**standby *4095* preempt**

Router1(config-if)#**end**

Router1#

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**interface *FastEthernet0/0***

Router2(config-if)#**standby version 2**

Router2(config-if)#**standby *4095* ip *10.1.1.1***

Router2(config-if)#**standby *4095* timers msec *15* msec *50***

Router2(config-if)#**standby *4095* priority *150***

Router2(config-if)#**standby *4095* preempt**

Router2(config-if)#**end**

Router2#

注释 从 12.3(4)T 后开始支持 HSRPv2，主要是扩展了可用组数，从 v1 的 256 个组到现在的 4095 个组，使用不同的 MAC 地址和组播地址，因此不能混用

22.13.   VRRP

提问 在思科路由器上启用 VRRP

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *FastEthernet0/1***

Router1(config-if)#**ip address *10.1.1.2 255.255.255.0***

Router1(config-if)#**vrrp *1* ip *10.1.1.1***

Router1(config-if)#**vrrp *1* preempt**

Router1(config-if)#**vrrp *1* priority *200***

Router1(config-if)#**end**

Router1#

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**interface *FastEthernet0/0***

Router2(config-if)#**ip address *10.1.1.3 255.255.255.0***

Router2(config-if)#**vrrp *1* ip *10.1.1.1***

Router2(config-if)#**vrrp *1* preempt**

Router2(config-if)#**vrrp *1* priority *150***

Router2(config-if)#**end**

Router2#

注释 注意在鉴权的配置上如果思科和非思科设备搭配可能会有问题。在配置定时器上只能配置 Hello 间隔，可以在主路由器上配置，备份路由器可以通过配置 vrrp 1 timers learn 命令来自动学习，可以为配置添加描述，也支持 Track

22.14 GLBP

提问 配置 GLBP 来实现流量的自动负荷分担

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip address *172.22.1.3 255.255.255.0***

Router1(config-if)#**glbp *1* ip *172.22.1.1***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**interface *FastEthernet0/0***

Router2(config-if)#**ip address *172.22.1.2 255.255.255.0***

Router2(config-if)#**glbp *1* ip *172.22.1.1***

Router2(config-if)#**exit**

Router2(config)#**end**

Router2#

注释 GLBP 通过组内设备轮回的响应虚拟 MAC 地址来实现自动的负荷分担，当然也可以使用其他的分担方式，比如权重等，这样不需要通过配置多 HSRP 组的方式实现了均衡，并且所有设备使用同一的网关地址

第二十三章 IP 组播

23.1. 配置 PIM-DM 下的组播

提问 配置路由器基本的组播功能

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip multicast-routing**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip address *192.168.1.1 255.255.255.0***

Router1(config-if)#**ip pim dense-mode**

Router1(config-if)#**exit**

Router1(config)#**interface *Serial1/0***

Router1(config-if)#**ip address *192.168.2.5 255.255.255.252***

Router1(config-if)#**ip pim dense-mode**

Router1(config-if)#**end**

Router1#

Router2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router2(config)#**ip multicast-routing**

Router2(config)#**interface *FastEthernet0/0***

Router2(config-if)#**ip address *192.168.3.1 255.255.255.0***

Router2(config-if)#**ip pim dense-mode**

Router2(config-if)#**exit**

Router2(config)#**interface *Serial1/0***

Router2(config-if)#**ip address *192.168.2.6 255.255.255.252***

Router2(config-if)#**ip pim dense-mode**

Router2(config-if)#**end**

Router2#

注释 密集模式适合于组播发送方和接收方近距离的情况，发送方很少但是接收方数量很大。

23.2. 配置 PIM-SM 和 BSR 下的组播路由

提问 配置稀疏模式下的组播路由，使用 BSR 来分发 RP 信息

回答

参与组播的正常路由器

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip multicast-routing**

Router1(config)#**ip pim rp-address *192.168.15.5***

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip address *192.168.1.1 255.255.255.0***

Router1(config-if)#**ip pim sparse-mode**

Router1(config-if)#**interface *Serial1/0***

Router1(config-if)#**ip address *192.168.2.5 255.255.255.252***

Router1(config-if)#**ip pim sparse-mode**

Router1(config-if)#**end**

Router1#

RP 候选路由器和 BSR 候选路由器

Router-RP1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-RP1(config)#**ip multicast-routing**

Router-RP1(config)#**interface Loopback0**

Router-RP1(config-if)#**ip address *192.168.12.1 255.255.255.255***

Router-RP1(config-if)# **ip pim sparse-mode**

Router-RP1(config-if)#**exit**

Router-RP1(config)#**interface *FastEthernet0/0***

Router-RP1(config-if)#**ip address *192.168.1.1 255.255.255.0***

Router-RP1(config-if)#**ip pim sparse-mode**

Router-RP1(config-if)#**exit**

Router-RP1(config)#**interface *Serial1/0***

Router-RP1(config-if)#**ip address *192.168.2.5 255.255.255.252***

Router-RP1(config-if)#**ip pim sparse-mode**

Router-RP1(config-if)#**exit**

Router-RP1(config)#**ip pim rp-address *192.168.12.1 15***

Router-RP1(config)#**ip pim rp-candidate** ***loopback0*** **group-list** ***15***

Router-RP1(config)#**ip pim bsr-candidate** ***loopback0 1***

Router-RP1(config)#**access-list** ***15*** **permit** ***239.5.5.0 0.0.0.255***

Router-RP1(config)#**access-list** ***15*** **deny any**

Router-RP1(config)#**end**

Router-RP1#

注释 对于稀疏模式需要配置一个汇集点 Rendezvous Point (RP)来作为组播最短路径树 Shortest Path Trees (SPT)的根。配置路由器使用 RP 有两种方法，一种是 Router1 使用的静态指定的方式 **ip pim rp-address** ***192.168.15.5*** 另一种就是动态的发现 RP，这又有两种方式来实现，第一种是思科专有的 Auto-RP,另一种就是本例中的 Bootstrap Router。在 Router-RP1 中首先使用 **ip pim rp-candidate** 来宣告自己为可能 RP，然后使用 **ip pim bsr-candidate** 来配置为 Bootstrap Router (BSR).BSR 目的就是发布网络中所有可能的 RP 信息。另外需要指出的是建议还要配置 **ip pim rp-address** ***192.168.12.1 15*** 尤其是在 12.3 以后的 IOS。BSR 模式需要 PIM-SM v2 支持。

23.3. 配置 PIM-SM 和 AUTO-RP 下的组播路由

提问 配置稀疏模式下的组播路由，使用 Auto-RP 来分发 RP 信息

回答

参与组播的正常路由器

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip multicast-routing**

Router1(config)#**ip pim rp-address** ***192.168.15.5***

Router1(config)#**interface** ***FastEthernet0/0***

Router1(config-if)#**ip address** ***192.168.1.1 255.255.255.0***

Router1(config-if)#**ip pim sparse-dense-mode**

Router1(config-if)#**exit**

Router1(config)#**interface *Serial1/0***

Router1(config-if)#**ip address *192.168.2.5 255.255.255.252***

Router1(config-if)#**ip pim sparse-dense-mode**

Router1(config-if)#**end**

Router1#

候选 RP 路由器

Router-RP1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-RP1(config)#**ip multicast-routing**

Router-RP1(config)#**interface Loopback0**

Router-RP1(config-if)#**ip address *192.168.12.1 255.255.255.255***

Router-RP1(config-if)#**ip pim sparse-dense-mode**

Router-RP1(config-if)#**exit**

Router-RP1(config)#**interface *FastEthernet0/0***

Router-RP1(config-if)#**ip address *192.168.1.1 255.255.255.0***

Router-RP1(config-if)#**ip pim sparse-dense-mode**

Router-RP1(config-if)#**exit**

Router-RP1(config)#**interface *Serial1/0***

Router-RP1(config-if)#**ip address *192.168.2.5 255.255.255.252***

Router-RP1(config-if)#**ip pim sparse-dense-mode**

Router-RP1(config-if)#**exit**

Router-RP1(config)#**ip pim send-rp-announce *loopback0* scope *16* group-list *15***

Router-RP1(config)#**ip pim send-rp-discovery scope *16***

Router-RP1(config)#**access-list *15* permit *239.5.5.0 0.0.0.255***

Router-RP1(config)#**access-list *15* deny any**

Router-RP1(config)#**end**

Router-RP1#

注释 在 Auto-RP 方式下，增加了 **sparse-dense-mode** 模式，使用了专有的 224.0.1.39 和 224.0.1.40. 两个组播地址

23.4. 过滤 PIM 邻居

提问 防止路由器从其他设备接收到 PIM 数据包

回答

在 R1 上配置过滤对 R2

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip multicast-routing**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip address *192.168.1.1 255.255.255.0***

Router1(config-if)#**ip pim sparse-mode**

Router1(config-if)#**ip pim neighbor-filter *18***

Router1(config-if)#**exit**

Router1(config)#**access-list *18* deny any**

Router1(config)#**end**

Router1#

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**ip multicast-routing**

Router2(config)#**interface** ***FastEthernet0/0***

Router2(config-if)#**ip address** ***192.168.1.2 255.255.255.0***

Router2(config-if)#**ip pim dense-mode**

Router2(config-if)#**ip igmp helper-address** ***192.168.1.1***

Router2(config-if)#**end**

Router2#

注释 对 PIM 邻居的过滤除了可以实现安全以外，还可以做到 Multicast stub routing

23.5. 低频度组播包应用的支持

提问 配置对于低频度组播包应用的支持

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip multicast-routing**

Router1(config)#**ip pim spt-threshold** ***10*** **group-list** ***15***

Router1(config)#**access-list** ***15*** **permit** ***239.5.5.55***

Router1(config)#**access-list** ***15*** **deny any**

Router1(config)#**interface** ***FastEthernet0/0***

Router1(config-if)#**ip address *192.168.1.1 255.255.255.0***

Router1(config-if)#**ip pim sparse-dense-mode**

Router1(config-if)#**exit**

Router1(config)#**interface *Serial1/0***

Router1(config-if)#**ip address *192.168.2.5 255.255.255.252***

Router1(config-if)#**ip pim sparse-mode**

Router1(config-if)#**end**

Router1#

注释 对于那些发送组播数据包小，间隔长的应用需要使用稀疏模式，同时通过配置 SPT 阀值来保持所生成的组播路径树

23.6. 在 FRAME RELAY 或者 ATM 网络中使用组播

提问 在 NBMA 网络中使用 PIM-SM

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip multicast-routing**

Router1(config)#**interface Serial0/0**

Router1(config-if)#**encapsulation frame-relay**

Router1(config-if)#**ip pim sparse-mode**

Router1(config-if)#**ip pim nbma-mode**

Router1(config-if)#**end**

Router1#

注释 对于通常的 NBMA 网络中的 NBMA 接口无法区分下联不同接口的组播请求，通过 ip pim nbma-mode 命令来各自邻居的组播请求

23.7. 配置 CGMP

提问 配置路由器和 Catalyst 交换机之间使用 CGMP 通讯

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip multicast-routing**

Router1(config)#**interface FastEthernet0/0**

Router1(config-if)#**ip pim sparse-dense-mode**

Router1(config-if)#**ip cgmp**

Router1(config-if)#**end**

Router1#

注释 不同交换机上启用 CGMP 的命令可能不同，也不是所有的交换机都支持 CGMP

23.8. 使用 IGMP 版本 3

提问 配置 IGMPv3

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip multicast-routing**

Router1(config)#**ip pim ssm default**

Router1(config)#**interface FastEthernet0/0**

Router1(config-if)#**ip pim sparse-dense-mode**

Router1(config-if)#**ip igmp version 3**

Router1(config-if)#**end**

Router1#

如果想使用 Source-Specific Multicast(SSM)特性，但是终端设备不支持 v3，可以使用思科的 IGMP v3lite

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip multicast-routing**

Router1(config)#**ip pim ssm default**

Router1(config)#**interface FastEthernet0/0**

Router1(config-if)#**ip pim sparse-dense-mode**

Router1(config-if)#**ip igmp v3lite**

Router1(config-if)#**end**

Router1#

注释 v3 里面最有用的特性就是 SSM，不但可以指定想要接收的组播组，还可以指定组播源

23.9. 静态组播路由和组成员

提问 使用静态条目来取代动态的组播路由和组成员

回答

静态组播路由:

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip multicast-routing**

Router1(config)#**ip mroute *192.168.15.0 255.255.255.0 192.168.98.6***

Router1(config)#**interface Tunnel0**

Router1(config-if)#**ip address *192.168.98.5 255.255.255.252***

Router1(config-if)#**ip pim sparse-dense-mode**

Router1(config-if)#**tunnel mode gre ip**

Router1(config-if)#**end**

Router1#

静态组成员

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip multicast-routing**

Router1(config)#**interface FastEthernet0/0**

Router1(config-if)#**ip pim sparse-dense-mode**

Router1(config-if)#**ip igmp join-group *239.5.5.55***

Router1(config-if)#**end**

Router1#

注释 在 12.3(2)T 后引入了相近的 ip igmp join-group 命令，好处是此命令使用 fast switching 来处理组播包

23.10. 启用 MOSPF 来进行组播路由

提问 使用 MOSPF 来分发组播路由表

回答 思科不支持 MOSPF

23.11. 启用 DVMRP 来进行组播路由

提问 配置 DVMRP 来支持组播路由

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip multicast-routing**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip pim sparse-dense-mode**

Router1(config-if)#**ip dvmrp unicast-routing**

Router1(config-if)#**ip dvmrp summary-address *192.168.0.0 255.255.0.0***

Router1(config-if)#**end**

Router1#

注释 思科对 DVMRP 的支持也不是全面的，更多的是作为 DVMRP 和 PIM 之间的网关，而目前网络中很少有 DVMRP 的部署，推荐使用 PIM，PIM 使用的是单播的路由表，而 DVMRP 是自己维护一个组播路由表，使用 224.0.0.4 这个组播地址来交换邻居信息

23.12. DVMRP 隧道

提问 建立 DVMRP 隧道来穿越不支持组播的网络

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip multicast-routing**

Router1(config)#**interface Tunnel0**

Router1(config-if)#**ip unnumbered *FastEthernet0/0***

Router1(config-if)#**ip pim sparse-dense-mode**

Router1(config-if)#**ip dvmrp unicast-routing**

Router1(config-if)#**tunnel source *FastEthernet0/0***

Router1(config-if)#**tunnel destination *192.168.99.15***

Router1(config-if)#**tunnel mode dvmrp**

Router1(config-if)#**exit**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip address *192.168.1.1 255.255.255.0***

Router1(config-if)#**ip pim sparse-dense-mode**

Router1(config-if)#**end**

Router1#

注释 DVMRP 隧道是建立在思科路由器和传统的支持 DVMRP 的设备上，两台思科设备之间不支持这种隧道，这种隧道只能封装的是组播包，隧道接口和源接口都必须启用 PIM。

23.13. 配置双向 PIM（CONFIGURING BIDIRECTIONAL PIM）

提问 配置网络对双向 PIM 的支持

回答

RP 路由器

Router-RP1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router-RP1(config)#**ip multicast-routing**

Router-RP1(config)#**ip pim bidir-enable**

Router-RP1(config)#**ip pim rp-address** ***192.168.12.1*** **bidir**

Router-RP1(config)#**ip pim rp-candidate** ***Loopback0*** **group-list 15 bidir**

Router-RP1(config)#**ip pim bsr-candidate** ***Loopback0 1***

Router-RP1(config)#**access-list** ***15*** **permit** ***239.5.5.0 0.0.0.255***

Router-RP1(config)#**access-list** ***15*** **deny any**

Router-RP1(config)#**interface Loopback0**

Router-RP1(config-if)#**ip address** ***192.168.12.1 255.255.255.255***

Router-RP1(config-if)# **ip pim sparse-mode**

Router-RP1(config-if)#**exit**

Router-RP1(config)#**interface** ***FastEthernet0/0***

Router-RP1(config-if)#**ip address** ***192.168.1.1 255.255.255.0***

Router-RP1(config-if)#**ip pim sparse-mode**

Router-RP1(config-if)#**exit**

Router-RP1(config)#**interface** ***Serial1/0***

Router-RP1(config-if)#**ip address** ***192.168.2.5 255.255.255.252***

Router-RP1(config-if)#**ip pim sparse-mode**

Router-RP1(config-if)#**exit**

Router-RP1(config)#**end**

Router-RP1#

其他路由器

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip multicast-routing**

Router1(config)#**ip pim bidir-enable**

Router1(config)#**ip pim rp-address *192.168.12.1*** bidir

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip address *192.168.1.2 255.255.255.0***

Router1(config-if)#**ip pim sparse-mode**

Router1(config-if)#**interface *Serial1/0***

Router1(config-if)#**ip address *192.168.3.5 255.255.255.252***

Router1(config-if)#**ip pim sparse-mode**

Router1(config-if)#**end**

Router1#

注释 双向 PIM 类似 PIM-SM，但是在机理上稍微有所不同，如果要部署双向 PIM 一定要在全网路由器上都配置支持，版本都要在 12.2 以上

23.14. 使用 TTL 来控制组播范围

提问 确保组播只作用于特定的网络范围

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip multicast-routing**

Router1(config)#**interface FastEthernet0/0**

Router1(config-if)#**ip multicast ttl-threshold *16***

Router1(config-if)#**end**

Router1#

注释 这里的配置更多取决于组播服务器对 TTL 的定义，通常本地 TTL 为 1，部门为 16，企业为 64，互联网为 128。另外跟单播不同的是，如果 TTL 超期被丢弃不会返回 ICMP TTL 超时的错误消息

23.15. 使用 ADMINISTRATIVELY SCOPED ADDRESSING 来控制组播范围

提问 使用 RFC2365 中定义的管理范围地址来控制组播的分发

回答

```
Router1#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router1(config)#ip multicast-routing
Router1(config)#access-list 15 deny 239.255.0.0 0.0.255.255
Router1(config)#access-list 15 permit any
Router1(config)#interface FastEthernet0/0
Router1(config-if)#ip multicast boundary 15
Router1(config-if)#end
Router1#
```

注释 由于使用 TTL 来控制更多依赖于组播应用，所以使用了上例的控制方法，针对 239.0.0.0 到 239.255.255.255 的组播地址，不同的应用和范围使用不同的地址段，对地址段进行控制。这里的命令不同于在端口配置简单的过滤列表，还对 PIM 的消息进行了控制，从而防止加入组播树

23.16. 使用 MBGP 来交换组播路由信息

提问 使用 MBGP 在两个网络中互相交换组播路由信息

回答

首先在 ASBR 上启用组播路由和对本地组播进行过滤

Router-ASBR1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-ASBR1(config)#**ip multicast-routing**

Router-ASBR1(config)#**access-list *15* deny 239.0.0.0 0.255.255.255**

Router-ASBR1(config)#**access-list *15* deny 224.0.1.39**

Router-ASBR1(config)#**access-list *15* deny 224.0.1.40**

Router-ASBR1(config)#**access-list *15* permit any**

Router-ASBR1(config)#**interface Serial0/0**

Router-ASBR1(config-if)#**ip multicast boundary *15***

Router-ASBR1(config-if)#**ip multicast ttl-threshold 64**

Router-ASBR1(config-if)#**ip pim dense-mode**

Router-ASBR1(config-if)#**end**

Router-ASBR1#

然后配置 MBGP

Router-ASBR1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-ASBR1(config)#**router bgp *65530***

Router-ASBR1(config-router)#**network *10.0.0.0* mask *255.0.0.0***

Router-ASBR1(config-router)#**neighbor *10.15.32.1* remote-as *65531***

Router-ASBR1(config-router)#**address-family ipv4 multicast**

Router-ASBR1(config-router-af)#**neighbor *10.15.32.1* activate**

Router-ASBR1(config-router-af)#**end**

Router-ASBR1#

注释 MBGP 并不像 PIM 一样是一种组播路由协议，只是用来传递路由信息，所以在配置中还有 PIM 的配置

23.17. 使用 MSDP 来发现外部源

提问 使用 MSDP 来发现另一个自治域的组播源

回答

Router-ASBR1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router-ASBR1(config)#**ip multicast-routing**

Router-ASBR1(config)#**interface Loopback0**

Router-ASBR1(config-if)#**ip address *192.168.12.1 255.255.255.255***

Router-ASBR1(config-if)# **ip pim sparse-mode**

Router-ASBR1(config-if)#**interface *FastEthernet0/0***

Router-ASBR1(config-if)#**ip address *192.168.1.1 255.255.255.0***

Router-ASBR1(config-if)#**ip pim sparse-mode**

Router-ASBR1(config-if)#**exit**

Router-ASBR1(config)#**interface *Serial1/0***

Router-ASBR1(config-if)#**ip address *192.168.2.5 255.255.255.252***

Router-ASBR1(config-if)#**ip multicast boundary *15***

Router-ASBR1(config-if)#**ip multicast ttl-threshold 64**

Router-ASBR1(config-if)#**ip pim sparse-mode**

Router-ASBR1(config-if)#**exit**

Router-ASBR1(config)#**ip pim rp-candidate *loopback0***

Router-ASBR1(config)#**ip pim bsr-candidate *loopback0 1***

Router-ASBR1(config-if)#**router bgp *65530***

Router-ASBR1(config-router)#**network *10.0.0.0* mask *255.0.0.0***

Router-ASBR1(config-router)#**neighbor *192.168.2.6* remote-as *65531***

Router-ASBR1(config-router)#**address-family ipv4 multicast**

Router-ASBR1(config-router-af)#**neighbor *192.168.2.6* activate**

Router-ASBR1(config-router-af)#**exit**

Router-ASBR1(config-router)#**exit**

Router-ASBR1(config)#**ip msdp peer *192.168.2.6***

Router-ASBR1(config)#**ip msdp sa-request *192.168.2.6***

Router-ASBR1(config)#**access-list *15* deny 239.0.0.0 0.255.255.255**

Router-ASBR1(config)#**access-list *15* deny 224.0.1.39**

Router-ASBR1(config)#**access-list *15* deny 224.0.1.40**

Router-ASBR1(config)#**access-list *15* permit any**

Router-ASBR1(config)#**end**

Router-ASBR1#

注释 这里面主要是配置了 sa 在对端来发布如果有新源的消息

23.18. 配置 ANYCAST RP

提问 配置两个或者多个 RP 来让路由器自动选择最近的

回答

第一个 RP 的配置

Router-RP1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-RP1(config)#**ip multicast-routing**

Router-RP1(config)#**interface Loopback0**

Router-RP1(config-if)# **ip address *10.4.4.4 255.255.255.255***

Router-RP1(config-if)#**exit**

Router-RP1(config)#**interface Loopback1**

Router-RP1(config-if)# **ip address *192.168.99.1 255.255.255.255***

Router-RP1(config-if)# **ip pim sparse-dense-mode**

Router-RP1(config-if)#**exit**

Router-RP1(config)#**ip pim send-rp-announce Loopback1 scope *16* group-list *22***

Router-RP1(config)#**ip pim send-rp-discovery Loopback1 scope *16***

Router-RP1(config)#**ip msdp peer *10.5.5.5* connect-source Loopback0**

Router-RP1(config)#**access-list *22* permit *239.0.0.0 0.255.255.255.255***

Router-RP1(config)#**end**

Router-RP1#

第二个 RP 的配置

Router-RP2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-RP2(config)#**ip multicast-routing**

Router-RP2(config)#**interface Loopback0**

Router-RP2(config-if)# **ip address** ***10.5.5.5 255.255.255.255***

Router-RP2(config-if)#**exit**

Router-RP2(config)#**interface Loopback1**

Router-RP2(config-if)# **ip address** ***192.168.99.1 255.255.255.255***

Router-RP2(config-if)# **ip pim sparse-dense-mode**

Router-RP2(config-if)#**exit**

Router-RP2(config)#**ip pim send-rp-announce Loopback1 scope** ***16*** **group-list** ***22***

Router-RP2(config)#**ip pim send-rp-discovery Loopback1 scope** ***16***

Router-RP2(config)#**ip msdp peer** ***10.4.4.4*** **connect-source Loopback0**

Router-RP2(config)#**access-list** ***22*** **permit** ***239.0.0.0 0.255.255.255.255***

Router-RP2(config)#**end**

Router-RP2#

注释 PIM-SM 有个缺陷就是在一个组播组里面只能有一个 RP，冗余性不够。而 Anycast 通过配置相同的 Anycast 地址，然后利用单播路由协议来保证采用最近的 RP，不同的 RP 之间可以利用 MSDP 来保证组播源的信息同步

23.19. 转化广播为组播

提问 把基于广播的应用转为组播包在网络中传递

回答

第一跳路由器

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip multicast-routing**

Router1(config)#**access-list *115* permit any any udp *3535***

Router1(config)#**access-list *115* deny any any udp**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip directed broadcast**

Router1(config-if)#**ip multicast helper-map broadcast *239.3.5.35 115***

Router1(config-if)#**exit**

Router1(config)#**ip pim sparse-dense-mode**

Router1(config)#**ip forward-protocol udp *3535***

Router1(config)#**end**

Router1#

最后一跳路由器

Router2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router2(config)#**ip multicast-routing**

Router2(config)#**access-list *115* permit any any udp *3535***

Router2(config)#**access-list *115* deny any any udp**

Router2(config)#**interface *Ethernet0***

Router2(config-if)#**ip address *192.168.9.1 255.255.255.0***

Router2(config-if)#**ip directed broadcast**

Router2(config-if)#**ip multicast helper-map *239.3.5.35 192.168.9.255 115***

Router2(config-if)#**ip pim sparse-dense-mode**

Router2(config-if)#**exit**

Router2(config)#**ip igmp join-group *239.3.5.35***

Router2(config)#**ip forward-protocol udp *3535***

Router2(config)#**end**

Router2#

注释 IP Multicast Helper 的特性帮助路由器实现了此种转换，但是此种转化比较耗费 CPU，仅仅是临时解决方案

23.20. 显示组播状态信息

提问 显示组播状态信息

回答

Router#**show ip mroute**

Router#**show ip mroute count**

Router#**show ip mroute active**

Router#**show ip igmp groups**

Router#**show ip igmp interface**

Router#**show ip pim neighbor**

Router#**show ip pim interface**

Router#**show ip pim rp**

Router#**show ip msdp count**

Router#**show ip msdp peer *192.168.201.15***

Router#**show ip msdp summary**

Router#**show ip rpf *192.168.3.2***

Router#**mstat *192.168.3.2 239.5.5.55***

注释 无

23.21. 组播路由排错

提问 组播路由排错

回答

Router#**debug ip mrouting**

Router#**debug ip mpacket *239.5.5.55***

Router#**debug ip igmp**

注释 无

第二十四章 移动 IP

24.1. 本地移动性（LOCAL AREA MOBILITY）

提问 配置本地移动性来实现设备的网络漫游

回答

归属地路由器 HomeRouter

RouterHome#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

RouterHome(config)#**interface *FastEthernet0/0***

RouterHome(config-if)#**ip address *192.168.10.1 255.255.255.0***

RouterHome(config-if)#**ip proxy-arp**

RouterHome(config-if)#**ip mobile arp**

RouterHome(config-if)#**exit**

RouterHome(config)#**router eigrp *99***

RouterHome(config-router)#**network** ***192.168.10.0***

RouterHome(config-router)#**default-metric** ***10000 10 255 1 1500***

RouterHome(config-router)#**redistribute mobile**

RouterHome(config-router)#**no auto-summary**

RouterHome(config-router)#**exit**

RouterHome(config)#end

RouterHome#

访问地路由器 ForeignRouter

RouterForeign#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

RouterForeign(config)#**interface** ***FastEthernet0/0***

RouterForeign(config-if)#**ip address** ***192.168.110.1 255.255.255.0***

RouterForeign(config-if)#**ip proxy-arp**

RouterForeign(config-if)#**ip mobile arp**

RouterForeign(config-if)#**exit**

RouterForeign(config)#**router eigrp** ***99***

RouterForeign(config-router)#**network** ***192.168.100.0***

RouterForeign(config-router)#**default-metric** ***10000 10 255 1 1500***

RouterForeign(config-router)#**redistribute mobile**

RouterForeign(config-router)#**no auto-summary**

RouterForeign(config-router)#**exit**

RouterForeign(config)#**end**

RouterForeign#

注释 Local Area Mobility 是思科通过 Proxy Arp 来实现的一种简单移动 IP，只是作为没有 DHCP 的暂时替代方案，当访问地使用 ARP 查到了访问设备以后会在路由表生成一条主机路由，然后此主机路由会通过路由协议被归属地所学到，比如访问地的 ARP 和路由表

RouterForeign#**show ip arp *FastEthernet0/0***

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.110.1	-	000e.d7d6.1060	ARPA	FastEthernet0/0
Internet	**192.168.10.109**	**1**	**00b0.64ab.0580**	**ARPA**	**FastEthernet0/0**
Internet	192.168.110.9	21	0000.0c75.c684	ARPA	FastEthernet0/0

RouterForeign#

RouterForeign#**show ip route**

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C      192.168.110.0/24 is directly connected, FastEthernet0/0
```

192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks

M 192.168.10.109/32 [3/1] via 192.168.10.109, 00:17:59, FastEthernet0/0

D 192.168.10.0/24 [90/2172416] via 192.168.55.11, 00:29:43, Serial0/0

C 192.168.55.0/24 is directly connected, Serial0/0

RouterForeign#

归属地通过 EIGRP 学到

RouterHome#**show ip route**

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default, U - per-user static route

o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

D 192.168.110.0/24 [90/2172416] via 192.168.55.12, 00:31:43, Serial0/0

192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks

D EX 192.168.10.109/32 [170/2172416] via 192.168.55.12, 00:18:19, Serial0/0

C 192.168.10.0/24 is directly connected, FastEthernet0/0

C 192.168.55.0/24 is directly connected, Serial0/0

RouterHome#

24.2. 归属地代理（HOME AGENT）配置

提问 配置路由器成为移动终端的归属地代理

回答

RouterHome#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

RouterHome(config)#**interface *Loopback0***

RouterHome(config-if)#**ip address *192.168.9.1 255.255.255.255***

RouterHome(config-if)#**exit**

RouterHome(config)#**router mobile**

RouterHome(config-router)#**exit**

RouterHome(config)#**router eigrp *99***

RouterHome(config-router)#**redistribute mobile**

RouterHome(config-router)#**network *192.168.9.0***

RouterHome(config-router)#**network *192.168.10.0***

RouterHome(config-router)#**default-metric *10000 10 255 1 1500***

RouterHome(config-router)#**no auto-summary**

RouterHome(config-router)#**exit**

RouterHome(config)#**ip mobile home-agent address *192.168.9.1***

RouterHome(config)#**ip mobile virtual-network *192.168.10.0 255.255.255.0***

RouterHome(config)#**ip mobile host *192.168.10.1 192.168.10.254* virtual-network *192.168.10.0 255.255.255.0***

RouterHome(config)#**ip mobile secure host *192.168.10.110* spi *100* key ascii *neoshi***

RouterHome(config)#**ip mobile secure host *192.168.10.111* spi *100* key ascii *neoshi***

RouterHome(config)#**ip mobile secure host *192.168.10.112* spi *100* key ascii *neoshi***

RouterHome(config)#**ip mobile secure host *192.168.10.113* spi *100* key ascii *neoshi***

RouterHome(config)#**ip mobile secure host *192.168.10.114* spi *100* key ascii *neoshi***

RouterHome(config)#**ip mobile secure host *192.168.10.115* spi *100* key ascii *neoshi***

RouterHome(config)#**end**

RouterHome#

注释 配置归属地代理是配置移动 IP 的第一步，首先是基本的移动 IP 配置然后是定义 Home Agent 的 IP 地址和定义移动终端的地址段，最后是配置对不同移动终端的认证，对于认证也可以使用 AAA 来增强扩展性

RouterHome(config)#**aaa new-model**

RouterHome(config)#**aaa authorization ipmobile default group tacacs+**

RouterHome(config)#**ip mobile secure mn-aaa spi *200* algorithm md5**

注意一点移动 IP 隧道使用的 IP 协议号是 55

24.3. 访问地代理（FOREIGN AGENT）配置

提问 配置路由器成为移动终端的访问地代理

回答

RouterForeign#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

RouterForeign(config)#**router mobile**

RouterForeign(config-router)#**exit**

RouterForeign(config)#**router eigrp** ***99***

RouterForeign(config-router)#**network** ***192.168.110.0***

RouterForeign(config-router)#**no auto-summary**

RouterForeign(config-router)#**exit**

RouterForeign(config)#**interface** ***Ethernet0/0***

RouterForeign(config-if)#**ip address** ***192.168.110.1 255.255.255.0***

RouterForeign(config-if)#**ip irdp**

RouterForeign(config-if)#**ip mobile foreign-service**

RouterForeign(config-if)#**exit**

RouterForeign(config)#**ip mobile foreign-agent care-of** ***Ethernet0/0***

RouterForeign(config)#**end**

RouterForeign#

注释 移动 IP 的第二步配置就是配置访问地代理，初始配置和归属地代理配置基本相同，然后就是在接口启用 IRDP，移动终端通过 IRDP 来发现访问地代理地址，然后启用归属地代理，最后是配置归属地的转交地址（*care-of* address）此地址用来和归属地地址建立隧道。有趣的是不论在归属地还是访问地的配置中都没有定义对端的地址，因为这个地址在移动终端会宣告。

另外为了增加安全性可以配置归属地代理和访问地代理的认证

RouterHome(config)#**ip mobile secure foreign-agent** ***192.168.110.1*** **spi** ***100*** **key ascii** ***neoshi***

RouterForeign(config)#**ip mobile secure home-agent** ***192.168.9.1*** **spi** ***100*** **key ascii** ***neoshi***

24.4. 配置路由器成为移动终端

提问 配置路由器作为移动终端

回答

RouterMobile#**configure terminal**

```
Enter configuration commands, one per line.    End with CNTL/Z.
RouterMobile(config)#router mobile
RouterMobile(config-router)#exit
RouterMobile(config)#ip mobile secure home-agent 192.168.9.1 spi 100 key ascii neoshi
RouterMobile(config)#ip mobile router
RouterMobile(mobile-router)#address 192.168.10.112 255.255.255.0
RouterMobile(mobile-router)#home-agent 192.168.9.1
RouterMobile(mobile-router)#exit
RouterMobile(config)#interface FastEthernet0/0
RouterMobile(config-if)#ip address 192.168.10.112 255.255.255.0
RouterMobile(config-if)#ip irdp
RouterMobile(config-if)#ip mobile router-service roam
RouterMobile(config-if)#ip mobile router-service solicit
RouterMobile(config-if)#exit
RouterMobile(config)#end
RouterMobile#
```

注释 从 12.2(4)T 以后路由器开始支持配置为移动终端

24.5. 反向隧道转发（REVERSE-TUNNEL FORWARDING）

提问 强制所有数据包都通过隧道转发来避免网络中为了防止地址欺骗所定义的控制列表

回答

```
RouterMobile#configure terminal
```

```
Enter configuration commands, one per line.    End with CNTL/Z.
RouterMobile(config)#ip mobile router
RouterMobile(mobile-router)#reverse-tunnel
RouterMobile(mobile-router)#exit
RouterMobile(config)#end
RouterMobile#
```

注释 由移动终端回程的数据包到了访问地代理后可能会通过本地路由而不是通过隧道转发回归属地代理，这样可能回违反访问地代理的安全策略，因此启用此特性来强制回程数据包也必须通过隧道转发，不过这个特性需要协商，验证：

```
RouterForeign#show ip mobile tunnel
Mobile Tunnels:

Tunnel0:
    src 192.168.110.1, dest 192.168.9.1
    encap IP/IP, mode reverse-allowed, tunnel-users 1
    IP MTU 1480 bytes
    Path MTU Discovery, mtu: 0, ager: 10 mins, expires: never
    outbound interface Serial0/0
    FA created, fast switching enabled, ICMP unreachable enabled
    105 packets input, 8462 bytes, 0 drops
    0 packets output, 0 bytes
RouterForeign#
```

24.6. 配置归属地代理 HSRP 支持来增加冗余性

提问 通过配置多个归属地代理来增加冗余

回答

RouterHome1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

RouterHome1(config)#**interface *FastEthernet0/0***

RouterHome1(config-if)#**ip address *192.168.9.2 255.255.255.0***

RouterHome1(config-if)#**standby *1* ip *192.168.9.1***

RouterHome1(config-if)#**standby *1* name *HA-GROUP***

RouterHome1(config-if)#**exit**

RouterHome1(config)#**router mobile**

RouterHome1(config-router)#**exit**

RouterHome1(config)#**router eigrp *99***

RouterHome1(config-router)#**redistribute mobile**

RouterHome1(config-router)#**network *192.168.9.0***

RouterHome1(config-router)#**network *192.168.10.0***

RouterHome1(config-router)#**default-metric *10000 10 255 1 1500***

RouterHome1(config-router)#**no auto-summary**

RouterHome1(config-router)#**exit**

RouterHome1(config)#**ip mobile home-agent address *192.168.9.1***

RouterHome1(config)#**ip mobile home-agent redundancy *HA-GROUP* virtual-network**

RouterHome1(config)#**ip mobile virtual-network *192.168.10.0 255.255.255.0***

RouterHome1(config)#**ip mobile host** ***192.168.10.1 192.168.10.254*** **virtual-network** ***192.168.10.0 255.255.255.0***

RouterHome1(config)#**ip mobile secure home-agent** ***192.168.9.3*** **spi** ***100*** **key ascii** ***cisco***

RouterHome1(config)#**ip mobile secure host** ***192.168.10.110*** **spi** ***100*** **key ascii** ***cookbook***

RouterHome1(config)#**ip mobile secure host** ***192.168.10.111*** **spi** ***100*** **key ascii** ***cookbook***

RouterHome1(config)#**ip mobile secure host** ***192.168.10.112*** **spi** ***100*** **key ascii** ***cookbook***

RouterHome1(config)#**ip mobile secure host** ***192.168.10.113*** **spi** ***100*** **key ascii** ***cookbook***

RouterHome1(config)#**ip mobile secure host** ***192.168.10.114*** **spi** ***100*** **key ascii** ***cookbook***

RouterHome1(config)#**ip mobile secure host** ***192.168.10.115*** **spi** ***100*** **key ascii** ***cookbook***

RouterHome1(config)#**end**

RouterHome1#

RouterHome2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

RouterHome2(config)#**interface** ***FastEthernet0/0***

RouterHome2(config-if)#**ip address** ***192.168.9.3 255.255.255.0***

RouterHome2(config-if)#**standby** ***1*** **ip** ***192.168.9.1***

RouterHome2(config-if)#**standby** ***1*** **name** ***HA-GROUP***

RouterHome2(config-if)#**exit**

RouterHome2(config)#**router mobile**

RouterHome2(config-router)#**exit**

RouterHome2(config)#**router eigrp** ***99***

RouterHome2(config-router)#**redistribute mobile**

RouterHome2(config-router)#**network** ***192.168.9.0***

RouterHome2(config-router)#**network** ***192.168.10.0***

RouterHome2(config-router)#**default-metric** ***10000 10 255 1 1500***

RouterHome2(config-router)#**no auto-summary**

RouterHome2(config-router)#**exit**

RouterHome2(config)#**ip mobile home-agent address** ***192.168.9.1***

RouterHome2(config)#**ip mobile home-agent redundancy** ***HA-GROUP*** **virtual-network**

RouterHome2(config)#**ip mobile virtual-network** ***192.168.10.0 255.255.255.0***

RouterHome2(config)#**ip mobile host** ***192.168.10.1 192.168.10.254*** **virtual-network** ***192.168.10.0 255.255.255.0***

RouterHome2(config)#**ip mobile secure home-agent** ***192.168.9.2*** **spi** ***100*** **key ascii** ***cisco***

RouterHome2(config)#**ip mobile secure host** ***192.168.10.110*** **spi** ***100*** **key ascii** ***cookbook***

RouterHome2(config)#**ip mobile secure host** ***192.168.10.111*** **spi** ***100*** **key ascii** ***cookbook***

RouterHome2(config)#**ip mobile secure host** ***192.168.10.112*** **spi** ***100*** **key ascii** ***cookbook***

RouterHome2(config)#**ip mobile secure host** ***192.168.10.113*** **spi** ***100*** **key ascii** ***cookbook***

RouterHome2(config)#**ip mobile secure host** ***192.168.10.114*** **spi** ***100*** **key ascii** ***cookbook***

RouterHome2(config)#**ip mobile secure host** ***192.168.10.115*** **spi** ***100*** **key ascii** ***cookbook***

RouterHome2(config)#**end**

RouterHome2#

注释 使用 HSRP 的虚拟地址来作为归属地地址来增加冗余，另外多了 **ip mobile home-agent redundancy** ***HA-GROUP*** **virtual-network** 命令来关联相应的 HSRP 组，同时需要配置两个归属地代理之间的认证来同步信息 **ip mobile secure home-agent** ***192.168.9.3*** **spi** ***100*** **key ascii** ***cisco***

第二十五章 IPV6

25.1. 自动配置接口 IPV6 地址

提问 在接口启用 IPv6，自动生成 IPv6 地址

回答

一种是使用 autoconfig 方式

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ipv6 unicast-routing**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ipv6 address autoconfig**

Router1(config-if)#**end**

Router1#

一种是使用 EUI-64 方式 来生成 IPv6 地址的主机部分，然后组合已定义的网络部分

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ipv6 unicast-routing**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ipv6 address *AAAA::/64* eui-64**

Router1(config-if)#**end**

Router1#

注释 ipv6 unicast-routing 命令是用来启动路由协议，尽管不用该命令你一样可以配置 v6 地址，也可以使用 v6 的 Ping 等命令，甚至配置静态路由来联通网络，但是还是建议配置此命令。对于 autoconfig 方式一是会自动生成前缀为 FE80::/10 的 linklocal 地址另外会查询 DHCP 来获的地址。对于 EUI 方式会根据 MAC 地址来生成前缀为 AAAA::/64 Global Unicast 地址

25.2. 手动配置接口 IPV6 地址

提问 手动给接口配置 IPv6 地址

回答

配置 Unicast 地址:

```
Router1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#ipv6 unicast-routing
Router1(config)#interface FastEthernet0/0
Router1(config-if)#ipv6 address AAAA::1/64
Router1(config-if)#exit
Router1(config)#end
Router1#
```

配置 Anycast 地址

```
Router1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router1(config)#ipv6 unicast-routing
Router1(config)#interface FastEthernet0/0
Router1(config-if)#ipv6 address AAFF::1/64 anycast
Router1(config-if)#exit
Router1(config)#end
Router1#
```

配置 link-local 地址

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ipv6 unicast-routing**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ipv6 address FE80::1 link-local**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 配置了 unicast 地址会自动根据 EUI 方式生成 Linklocal 地址。Anycast 在 root dns 遭受攻击中发挥了很大作用，看一个命令输出

Router1#**show ipv6 interface *FastEthernet0/0***

FastEthernet0/0 is up, line protocol is up

IPv6 is enabled, link-local address is FE80::20E:84FF:FE24:4E70

Global unicast address(es):

AAAA::1, subnet is AAAA::/64

AAFF::1, subnet is AAFF::/64 [ANY]

Joined group address(es):

FF02::1

FF02::2

FF02::1:FF00:1

FF02::1:FF24:4E70

MTU is 1500 bytes

ICMP error messages limited to one every 100 milliseconds

ICMP redirects are enabled

ND DAD is enabled, number of DAD attempts: 1

ND reachable time is 30000 milliseconds

ND advertised reachable time is 0 milliseconds

ND advertised retransmit interval is 0 milliseconds

ND router advertisements are sent every 200 seconds

ND router advertisements live for 1800 seconds

Hosts use stateless autoconfig for addresses.

Router1#

25.3. 配置 IPV6 DHCP 服务

提问 在路由器上启用 DHCP 服务器特性来提供 IPv6 地址

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ipv6 dhcp database *flash:/DHCPv6-db***

Router1(config)#**ipv6 local pool *VLAN10-pool AAAA:1::/48 64***

Router1(config)#**ipv6 local pool *VLAN11-pool AAAA:11::/48 64***

Router1(config)#**ipv6 dhcp pool *DHCPv6POOL***

Router1(config-dhcp)#**prefix-delegation *AAAA:1::23F6:33BA/64 00030001000E84244E70***

Router1(config-dhcp)#**prefix-delegation pool *VLAN10-pool***

```
Router1(config-dhcp)#dns-server AAAA:1::19

Router1(config-dhcp)#domain-name oreilly.com

Router1(config-dhcp)#exit

Router1(config)#interface FastEthernet0/0

Router1(config-if)#ipv6 address AAAA:1::1/64

Router1(config-if)#ipv6 address FE80::1 link-local

Router1(config-if)#ipv6 nd managed-config-flag

Router1(config-if)#ipv6 nd other-config-flag

Router1(config-if)#ipv6 dhcp server DHCPv6POOL rapid-commit preference 1 allow-hint

Router1(config-if)#exit

Router1(config)#end

Router1#
```

注释 此特性仅限于高端路由器

```
Router1#show ipv6 dhcp pool DHCPv6POOL

DHCPv6 pool: DHCPv6POOL

  Static bindings:

    Binding for client 00030001000E84244E70

      IA PD: IA ID not specified

        Prefix: AAAA:1::23F6:33BA/64

                preferred lifetime 604800, valid lifetime 2592000

  Prefix pool: VLAN10-pool

               preferred lifetime 604800, valid lifetime 2592000
```

DNS server: AAAA:1::19

Domain name: oreilly.com

Active clients: 0

Router1#

25.4. 配置 RIP 的 IPV6 版本

提问 配置支持 IPv6 路由的 RIP

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ipv6 unicast-routing**

Router1(config)#**ipv6 router rip *RIP_PROC***

Router1(config-rtr)#**exit**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ipv6 address *AAAA:5:1/64***

Router1(config-if)#**ipv6 rip *RIP_PROC* enable**

Router1(config-if)#**exit**

Router1(config)#**interface *Serial0/0***

Router1(config-if)#**ipv6 address *AAAA:1:2/64***

Router1(config-if)#**ipv6 rip *RIP_PROC* enable**

Router1(config-if)#**frame-relay map ipv6 *AAAA:1:3 206* broadcast**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 ipv6 版本的 RIP 区别在于不需要配置 network 命令，在路由表中看到的下一跳地址都是 linklocal 地址：

Router1#**show ipv6 route rip**

IPv6 Routing Table - 9 entries

Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP

U - Per-user Static route

I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary

O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2

ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2

R AAAA:2::/64 [120/2]

via FE80::2E0:1EFF:FE7F:9E41, FastEthernet0/0

R AAAA:95::/64 [120/2]

via FE80::2E0:1EFF:FE7F:9E41, FastEthernet0/0

R AAAA:99::/64 [120/2]

via FE80::20E:D7FF:FED6:1060, FastEthernet0/0

Router1#

还有一个比较好用的命令

Router1#**show ipv6 rip next-hops**

RIP process "RIP_PROC", Next Hops

FE80::2E0:1EFF:FE7F:9E41/FastEthernet0/0 [2 paths]

FE80::20E:D7FF:FED6:1060/FastEthernet0/0 [7 paths]

FE80::200:CFF:FE75:C684/FastEthernet0/0 [2 paths]

FE80::2E0:1EFF:FE7F:9E41/Serial0/0 [2 paths]

Router1#

25.5. 修改 RIP 的缺省参数

提问 修改诸如定时器，管理距离等 RIP 参数

回答

修改定时器

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ipv6 unicast-routing**

Router1(config)#**ipv6 router rip *RIP_PROC***

Router1(config-rtr)#**timers *15 60 5 120***

Router1(config-rtr)#**exit**

Router1(config)#**end**

Router1#

修改管理距离

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ipv6 unicast-routing**

Router1(config)#**ipv6 router rip *RIP_PROC***

Router1(config-rtr)#**distance *100***

Router1(config-rtr)#**exit**

Router1(config)#**end**

Router1#

关闭水平分割

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ipv6 unicast-routing**

Router1(config)#**ipv6 router rip *RIP_PROC***

Router1(config-rtr)#**no split-horizon**

Router1(config-rtr)#**exit**

Router1(config)#**end**

Router1#

注释 思科并没有给 IPv6 版本和 v4 版本一样的可修改参数

Router1#**show ipv6 rip**

RIP process "RIP_PROC", port 521, multicast-group FF02::9, pid 125

Administrative distance is 120. Maximum paths is 16

Updates every 15 seconds, expire after 60

Holddown lasts 5 seconds, garbage collect after 120

Split horizon is on; poison reverse is off

Default routes are not generated

Periodic updates 755, trigger updates 3

Interfaces:

FastEthernet0/0

Loopback0

Redistribution:

None

Router1#

25.6. RIP 中 IPV6 路由的过滤和度量值的修改

提问 对 RIP 生成的路由表再加工

回答

地址汇总

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ipv6 rip *RIP_PROC* summary-address *AAAA:99::8:0/109***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

宣告缺省路由

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ipv6 rip *RIP_PROC* default-information originate**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ipv6 rip *RIP_PROC* default-information only**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

路由过滤

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ipv6 prefix-list *BLOCK_2E6* seq *5* deny *AAAA:2E6::/64* le *128***

Router1(config)#**ipv6 prefix-list *BLOCK_2E6* seq *10* permit ::/0 le 128**

Router1(config)#**ipv6 prefix-list *ALLOW_2222* seq *5* permit *AAAA:2222::/64* le *128***

Router1(config)#**ipv6 prefix-list *ALLOW_2222* seq *10* deny ::/0 le 128**

Router1(config)#**ipv6 router rip *RIP_PROC***

Router1(config-rtr)#**distribute-list prefix-list *BLOCK_2E6* in *FastEthernet0/0***

Router1(config-rtr)#**distribute-list prefix-list *ALLOW_2222* out *FastEthernet0/0***

Router1(config-rtr)#**exit**

Router1(config)#**end**

Router1#

修改度量值

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *Serial0/0***

Router1(config-if)#**ipv6 rip *RIP_PROC* metric-offset *5***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 基本配置方法和 IPv4 相同，在路由过滤的 Prefixlist 中 V6 只能接受 prefix list 的配置，后面不能跟 accesslist 作为参数

25.7. 配置 OSPF 的 IPV6 版本

提问 配置支持 IPv6 的 OSPF v3

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip cef**

Router1(config)#**ipv6 cef**

Router1(config)#**ipv6 unicast-routing**

Router1(config)#**ipv6 router ospf *1***

Router1(config-rtr)#**router-id *1.0.0.1***

Router1(config-rtr)#**area *0* range *AAAA:5::/64***

Router1(config-rtr)#**exit**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ipv6 address *AAAA:5::1/64***

Router1(config-if)#**ipv6 ospf *1* area *0***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 这里有个比较有意思的 router id 问题，在 v4 情况下会自动根据 IP 地址来选择，但是在纯 v6 环境下没有 v4 的地址，所以就必须配置 router id，否则 ospf 不能正常运行

25.8. OSPF 中 IPV6 路由过滤和度量值修改

提问 对 OSPF 生成的路由表再加工

回答

修改默认代价值

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ipv6 router ospf *1***

Router1(config-rtr)#**auto-cost reference-bandwidth *1000***

%OSPFv3: Reference bandwidth is change.

Please ensure reference bandwidth is consistent across all routers.

Router1(config-rtr)#**exit**

Router1(config)#**end**

Router1#

修改特定链路的代价值

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ipv6 ospf cost *500***

Router1(config)#**end**

Router1#

路由过滤

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ipv6 prefix-list *BLOCK_99_E* seq *5* deny *AAAA:99::E:0/112***

Router1(config)#**ipv6 prefix-list *BLOCK_99_E* seq *10* permit *::/0* le *128***

Router1(config)#**ipv6 router ospf *1***

Router1(config-rtr)#**distribute-list prefix-list *BLOCK_99_E* in**

Router1(config-rtr)#**exit**

Router1(config)#**end**

Router1#

注释 类似于 v4 的配置

25.9. 路由重分布

提问 不同路由协议之间进行再分布

回答

再分布 OSPF 到 RIP

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ipv6 router rip *RIP_PROC***

Router1(config-rtr)#**redistribute ospf *1* metric *5***

Router1(config-rtr)#**exit**

Router1(config)#**end**

Router1#

再分布 RIP 到 OSPF

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ipv6 router ospf *1***

Router1(config-rtr)#**redistribute rip *RIP_PROC***

Router1(config-rtr)#**exit**

Router1(config)#**end**

Router1#

OSPF 宣告缺省路由

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ipv6 router ospf *1***

Router1(config-rtr)#**default-information originate always**

Router1(config-rtr)#**exit**

Router1(config)#**end**

Router1#

注释 也可以使用 routemap 等高级方法

25.10. 配置 MBGP

提问 在不同的自治域系统使用 MBGP 来传递 IPv6 路由信息

回答

单 v6 环境

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**router bgp *65520***

Router1(config-router)#**no bgp default ipv4-unicast**

Router1(config-router)#**neighbor *AAAA:5::2* remote-as *65522***

Router1(config-router)#**neighbor *AAAA:5::AA9* remote-as *65521***

Router1(config-router)#**address-family ipv6**

Router1(config-router-af)#**neighbor *AAAA:5::2* activate**

Router1(config-router-af)#**neighbor *AAAA:5::AA9* activate**

Router1(config-router-af)#**network *AAAA:2222::2/64***

Router1(config-router-af)#**no synchronization**

Router1(config-router-af)#**exit-address-family**

Router1(config-router)#**exit**

Router1(config)#**end**

Router1#

V4 和 v6 混和环境

Router9#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router9(config)#**router bgp *65521***

Router9(config-router)#**no bgp default ipv4-unicast**

Router9(config-router)#**neighbor *AAAA:5::1* remote-as *65520***

Router9(config-router)#**neighbor *192.168.1.103* remote-as *65525***

Router9(config-router)#**address-family ipv4**

Router9(config-router-af)#**redistribute connected**

Router9(config-router-af)#**neighbor *192.168.1.103* activate**

Router9(config-router-af)#**no auto-summary**

Router9(config-router-af)#**no synchronization**

Router9(config-router-af)#**exit-address-family**

Router9(config-router)#**address-family ipv6**

Router9(config-router-af)#**neighbor *AAAA:5::1* activate**

Router9(config-router-af)#**network *AAAA:FE::1/64***

Router9(config-router-af)#**network *AAAA:BBBB::1/64***

Router9(config-router-af)#**no synchronization**

Router9(config-router-af)#**exit-address-family**

Router9(config-router)#**exit**

Router9(config)#**end**

Router9#

注释 和 V4 配置最大的不同是增加了 no bgp default ipv4-unicast 命令，因为缺省情况 BGP 只会发布 v4 的前缀给邻居。查看邻居状态使用 show bgp summary，而对于纯 v4 邻居使用的是 show ip bgp summary 命令

25.11. 在现有 IPV4 网络中传递 IPV6 数据

提问 通过现有的 IPv4 网络来互联两个 IPv6 网络

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**interface *Loopback1***

Router1(config-if)#**ip address *10.15.1.11 255.255.255.255***

Router1(config-if)#**exit**

Router1(config)#**interface *Tunnel1***

Router1(config-if)#**ipv6 address *BBBB:1::1/126***

Router1(config-if)#**ipv6 rip *RIP_PROC* enable**

Router1(config-if)#**tunnel source *10.15.1.11***

Router1(config-if)#**tunnel destination *172.16.11.9***

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

Router9#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router9(config)#**interface *Loopback1***

Router9(config-if)#**ip address *172.16.11.9 255.255.255.255***

Router9(config-if)#**exit**

Router9(config)#**interface *Tunnel1***

Router9(config-if)#**ipv6 address *BBBB:1::2/126***

Router9(config-if)#**ipv6 rip *RIP_PROC* enable**

Router9(config-if)#**tunnel source *172.16.11.9***

Router9(config-if)#**tunnel destination *10.15.1.11***

Router9(config-if)#**exit**

Router9(config)#**end**

Router9#

注释 这种 GRE 隧道的配置相比前面的例子要简单的多，问题也少很多，因为封装前后的协议类型是不同的

25.12.   IPV6 和 IPV4 之间转化

提问 配置路由器成为 IPv4 和 IPv 网络之间的网关

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ipv6 access-list *ALLOWED-NAT-DEVS***

Router1(config-ipv6-acl)# **permit ipv6 any any**

Router1(config-ipv6-acl)#**exit**

Router1(config)#**ipv6 nat prefix** ***::FFFF:0.0.0.0/96*** **v4-mapped** ***ALLOWED-NAT-DEVS***

Router1(config)#**ipv6 nat v6v4 source** ***AAAA:5::AA9 192.168.56.100***

Router1(config)#**interface** ***FastEthernet0/0***

Router1(config-if)#**no ip address**

Router1(config-if)#**ipv6 address** ***AAAA:5::2012/64***

Router1(config-if)#**ipv6 nat**

Router1(config-if)#**exit**

Router1(config)#**interface** ***Serial0/0***

Router1(config-if)#**ip address** ***192.168.55.12 255.255.255.0***

Router1(config-if)#**ipv6 nat**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 12.2(13)T 后路由器可以作为 v6 和 v4 之间的协议转化器，对于 v6 访问 v4 地址，可以采用 "IPv4-Mapped IPv6 Address" 把 a.b.c.d 翻译为::FFFF:A.B.C.D，而对于 v4 访问 v6 地址，只能采用静态映射的方式(**ipv6 nat v6v4**),这种地址翻译没有配置 inside 或者 outside 接口

第二十六章 MPLS

26.1. 配置基本的 MPLS P 路由器

提问 配置 MPLS 核心网络里面的 P 路由器

回答

Router-P1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router-P1(config)#**ip cef**

Router-P1(config)#**mpls ip**

Router-P1(config)#**interface *FastEthernet0/0***

Router-P1(config-if)#**description *connection to Router-PE2***

Router-P1(config-if)#**ip address *10.1.2.11 255.255.255.0***

Router-P1(config-if)#**mpls ip**

Router-P1(config-if)#**exit**

Router-P1(config)#**interface *Serial0/0***

Router-P1(config-if)#**description *connection to Router-PE1***

Router-P1(config-if)#**ip address *10.1.1.14 255.255.255.252***

Router-P1(config-if)#**mpls ip**

Router-P1(config-if)#**exit**

Router-P1(config)#**interface *Serial0/1***

Router-P1(config-if)#**description *connection to Router-PE3***

Router-P1(config-if)#**ip address *10.1.1.10 255.255.255.252***

Router-P1(config-if)#**mpls ip**

Router-P1(config-if)#**exit**

Router-P1(config)#**interface *Loopback0***

Router-P1(config-if)#**ip address *10.0.0.11 255.255.255.255***

Router-P1(config-if)#**exit**

Router-P1(config)#**router ospf *99***

Router-P1(config-router)#**router-id *10.0.0.11***

Router-P1(config-router)#**network *10.0.0.0 0.255.255.255* area *0***

Router-P1(config-router)#**exit**

Router-P1(config)#**end**

Router-P1#

注释 对于 P 路由器就是启用 CEF 和在端口启用 MPLS，对于 tag-switching ip instead 和 mpls ip 两个命令都基本一致，对于是否配置 ldp 或者 tdp 也不是必须的，路由器会自动适应。有三个验证命令：

Router-P1#**show mpls interfaces**

Interface	IP	Tunnel	Operational
FastEthernet0/0	Yes (tdp)	No	Yes
Serial0/0	Yes (tdp)	No	Yes
Serial0/1	Yes (tdp)	No	Yes

Router-P1#**show mpls ldp neighbor**

```
    Peer TDP Ident: 10.0.0.2:0; Local TDP Ident 10.0.0.11:0
        TCP connection: 10.0.0.2.711 - 10.0.0.11.28185
        State: Oper; PIEs sent/rcvd: 0/82; Downstream
        Up time: 01:04:45
        TDP discovery sources:
          Serial0/0, Src IP addr: 10.1.1.13
        Addresses bound to peer TDP Ident:
          10.0.0.2        10.1.1.2        10.1.1.13
```

Router-P1#**show mpls forwarding-table**

Local Outgoing Prefix Bytes tag Outgoing Next Hop

tag	tag or VC	or Tunnel Id	switched	interface	
16	Pop tag	10.0.0.2/32	7697	Se0/0	point2point
17	Pop tag	10.1.1.0/30	0	Se0/0	point2point
18	Pop tag	10.0.0.3/32	6685	Se0/1	point2point

26.2. 配置基本的 MPLS PE 路由器

提问 配置 MPLS 网络的运营商边界路由器来互联用户网络

回答

配置三台 PE 路由器

Router-PE1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router-PE1(config)#**ip cef**

Router-PE1(config)#**mpls ip**

Router-PE1(config)#**interface *Serial0/0***

Router-PE1(config-if)#**description *Connection to Router-P1***

Router-PE1(config-if)#**ip address *10.1.1.13 255.255.255.252***

Router-PE1(config-if)#**mpls ip**

Router-PE1(config-if)#**exit**

Router-PE1(config)#**interface *Loopback0***

Router-PE1(config-if)#**ip address *10.0.0.2 255.255.255.255***

Router-PE1(config-if)#**exit**

Router-PE1(config)#**router ospf *99***

Router-PE1(config-router)#**router-id** ***10.0.0.2***

Router-PE1(config-router)#**network** ***10.0.0.0 0.255.255.255*** **area** ***0***

Router-PE1(config-router)#**exit**

Router-PE1(config)#**ip vrf** ***NetworkA***

Router-PE1(config-vrf)#**rd** ***100:1***

Router-PE1(config-vrf)#**route-target export** ***100:1***

Router-PE1(config-vrf)#**route-target import** ***100:1***

Router-PE1(config-vrf)#**exit**

Router-PE1(config)#**ip vrf** ***NetworkB***

Router-PE1(config-vrf)#**rd** ***100:2***

Router-PE1(config-vrf)#**route-target export** ***100:2***

Router-PE1(config-vrf)#**route-target import** ***100:2***

Router-PE1(config-vrf)#**exit**

Router-PE1(config)#**interface** ***Ethernet0/0***

Router-PE1(config-if)#**description** ***connection to customer A, site 1***

Router-PE1(config-if)#**ip vrf forwarding** ***NetworkA***

Router-PE1(config-if)#**ip address** ***192.168.1.1 255.255.255.0***

Router-PE1(config-if)#**exit**

Router-PE1(config)#**interface** ***Ethernet0/1***

Router-PE1(config-if)#**description** ***connection to customer B, site 1***

Router-PE1(config-if)#**ip vrf forwarding** ***NetworkB***

Router-PE1(config-if)#**ip address** ***192.168.11.1 255.255.255.0***

Router-PE1(config-if)#**exit**

Router-PE1(config)#**router bgp *100***

Router-PE1(config-router)#**bgp log-neighbor-changes**

Router-PE1(config-router)#**neighbor *10.0.0.3* remote-as *100***

Router-PE1(config-router)#**neighbor *10.0.0.3* update-source *Loopback0***

Router-PE1(config-router)#**neighbor *10.0.0.4* remote-as *100***

Router-PE1(config-router)#**neighbor *10.0.0.4* update-source *Loopback0***

Router-PE1(config-router)#**address-family ipv4 vrf *NetworkA***

Router-PE1(config-router-af)#**no auto-summary**

Router-PE1(config-router-af)#**no synchronization**

Router-PE1(config-router-af)#**redistribute connected**

Router-PE1(config-router-af)#**exit-address-family**

Router-PE1(config-router)#**adress-family ipv4 vrf *NetworkB***

Router-PE1(config-router-af)#**no auto-summary**

Router-PE1(config-router-af)#**no synchronization**

Router-PE1(config-router-af)#**redistribute connected**

Router-PE1(config-router-af)#**exit-address-family**

Router-PE1(config-router)#**address-family vpnv4**

Router-PE1(config-router-af)#**neighbor *10.0.0.3* activate**

Router-PE1(config-router-af)#**neighbor *10.0.0.3* send-community extended**

Router-PE1(config-router-af)#**neighbor *10.0.0.4* activate**

Router-PE1(config-router-af)#**neighbor *10.0.0.4* send-community extended**

```
Router-PE1(config-router-af)#exit-address-family
Router-PE1(config-router)#exit
Router-PE1(config)#end
Router-PE1#
Router-PE2#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router-PE2(config)#ip cef
Router-PE2(config)#mpls ip
Router-PE2(config)#interface FastEthernet0/0
Router-PE2(config-if)#no ip address
Router-PE2(config-if)#exit
Router-PE2(config)#interface FastEthernet0/0.1
Router-PE2(config-if)#description Connection to Router-P1
Router-PE2(config-if)#encapsulation dot1Q 10
Router-PE2(config-if)#ip address 10.1.2.4 255.255.255.0
Router-PE2(config-if)#mpls ip
Router-PE2(config-if)#exit
Router-PE2(config)#interface Loopback0
Router-PE2(config-if)#ip address 10.0.0.3 255.255.255.255
Router-PE2(config-if)#exit
Router-PE2(config)#router ospf 99
Router-PE2(config-router)#router-id 10.0.0.3
```

Router-PE2(config-router)#**network *10.0.0.0 0.255.255.255* area *0***

Router-PE2(config-router)#**exit**

Router-PE2(config)#**ip vrf *NetworkA***

Router-PE2(config-vrf)#**rd *100:1***

Router-PE2(config-vrf)#**route-target export *100:1***

Router-PE2(config-vrf)#**route-target import *100:1***

Router-PE2(config-vrf)#**exit**

Router-PE2(config)#**ip vrf *NetworkB***

Router-PE2(config-vrf)#**rd *100:2***

Router-PE2(config-vrf)#**route-target export *100:2***

Router-PE2(config-vrf)#**route-target import *100:2***

Router-PE2(config-vrf)#**exit**

Router-PE2(config)#**interface *FastEthernet0/0.2***

Router-PE2(config-if)#**description *Connection to customer A, site 2***

Router-PE2(config-if)#**encapsulation dot1Q *102***

Router-PE2(config-if)#**ip address *192.168.3.1 255.255.255.0***

Router-PE2(config-if)#**mpls ip**

Router-PE2(config-if)#**exit**

Router-PE2(config)#**router bgp *100***

Router-PE2(config-router)#**bgp log-neighbor-changes**

Router-PE2(config-router)#**neighbor *10.0.0.2* remote-as *100***

Router-PE2(config-router)#**neighbor *10.0.0.2* update-source *Loopback0***

Router-PE2(config-router)#**neighbor *10.0.0.3* remote-as *100***

Router-PE2(config-router)#**neighbor *10.0.0.3* update-source *Loopback0***

Router-PE2(config-router)#**address-family ipv4 vrf *NetworkA***

Router-PE2(config-router-af)#**no auto-summary**

Router-PE2(config-router-af)#**no synchronization**

Router-PE2(config-router-af)#**redistribute connected**

Router-PE2(config-router-af)#**exit-address-family**

Router-PE2(config-router)#**address-family vpnv4**

Router-PE2(config-router-af)#**neighbor *10.0.0.2* activate**

Router-PE2(config-router-af)#**neighbor *10.0.0.2* send-community extended**

Router-PE2(config-router-af)#**neighbor *10.0.0.4* activate**

Router-PE2(config-router-af)#**neighbor *10.0.0.4* send-community extended**

Router-PE2(config-router-af)#**exit-address-family**

Router-PE2(config-router)#**exit**

Router-PE2(config)#**end**

Router-PE2#

Router-PE3#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-PE3(config)#**ip cef**

Router-PE3(config)#**mpls ip**

Router-PE3(config)#**interface *Serial0/0***

Router-PE3(config-if)#**description *Connection to Router-P1***

Router-PE3(config-if)#**ip address** ***10.1.1.9 255.255.255.252***

Router-PE3(config-if)#**mpls ip**

Router-PE3(config-if)#**exit**

Router-PE3(config)#**interface** ***Loopback0***

Router-PE3(config-if)#**ip address** ***10.0.0.3 255.255.255.255***

Router-PE3(config-if)#**exit**

Router-PE3(config)#**router ospf** ***99***

Router-PE3(config-router)#**router-id** ***10.0.0.3***

Router-PE3(config-router)#**network** ***10.0.0.0 0.255.255.255*** **area** ***0***

Router-PE3(config-router)#**exit**

Router-PE3(config)#**ip vrf** ***NetworkA***

Router-PE3(config-vrf)#**rd** ***100:1***

Router-PE3(config-vrf)#**route-target export** ***100:1***

Router-PE3(config-vrf)#**route-target import** ***100:1***

Router-PE3(config-vrf)#**exit**

Router-PE3(config)#**ip vrf** ***NetworkB***

Router-PE3(config-vrf)#**rd** ***100:2***

Router-PE3(config-vrf)#**route-target export** ***100:2***

Router-PE3(config-vrf)#**route-target import** ***100:2***

Router-PE3(config-vrf)#**exit**

Router-PE3(config)#**interface** ***Ethernet0/0***

Router-PE3(config-if)#**description** ***connection to customer A, site 3***

Router-PE3(config-if)#**ip vrf forwarding *NetworkA***

Router-PE3(config-if)#**ip address *192.168.2.1 255.255.255.0***

Router-PE3(config-if)#**exit**

Router-PE3(config)#**interface *Ethernet0/1***

Router-PE3(config-if)#**description *connection to customer B, site 2***

Router-PE3(config-if)#**ip vrf forwarding *NetworkB***

Router-PE3(config-if)#**ip address *192.168.10.1 255.255.255.0***

Router-PE3(config-if)#**exit**

Router-PE3(config)#**router bgp *100***

Router-PE3(config-router)#**bgp log-neighbor-changes**

Router-PE3(config-router)#**neighbor *10.0.0.2* remote-as *100***

Router-PE3(config-router)#**neighbor *10.0.0.2* update-source *Loopback0***

Router-PE3(config-router)#**neighbor *10.0.0.4* remote-as *100***

Router-PE3(config-router)#**neighbor *10.0.0.4* update-source *Loopback0***

Router-PE3(config-router)#**address-family ipv4 vrf *NetworkA***

Router-PE3(config-router-af)#**no auto-summary**

Router-PE3(config-router-af)#**no synchronization**

Router-PE3(config-router-af)#**redistribute connected**

Router-PE3(config-router-af)#**exit-address-family**

Router-PE3(config-router)#**adress-family ipv4 vrf *NetworkB***

Router-PE3(config-router-af)#**no auto-summary**

Router-PE3(config-router-af)#**no synchronization**

Router-PE3(config-router-af)#**redistribute connected**

Router-PE3(config-router-af)#**exit-address-family**

Router-PE3(config-router)#**address-family vpnv4**

Router-PE3(config-router-af)#**neighbor *10.0.0.2* activate**

Router-PE3(config-router-af)#**neighbor *10.0.0.2* send-community extended**

Router-PE3(config-router-af)#**neighbor *10.0.0.4* activate**

Router-PE3(config-router-af)#**neighbor *10.0.0.4* send-community extended**

Router-PE3(config-router-af)#**exit-address-family**

Router-PE3(config-router)#**exit**

Router-PE3(config)#**end**

Router-PE3#

注释 对于 PE 路由器首先是类似 P 路由器的基本 MPLS 配置，然后是配置了两个客户网络的 VRF，其中 rd 用来作为 MP BGP 发布此 VRF 路由的标签，route target 用来告诉 MP BGP 那个 rd 与之共享路由。在关联接口和 VRF 的时候要先配置 ip vrf forwarding 命令然后配置 IP 地址，通过 show ip vrf 来验证。然后就是 MP-BGP 的配置，这里和平常 BGP 配置最大的不同就是必须有 send-community extended 的配置，因为 VRF 的信息是通过这个值来宣告的，两个验证命令 show ip route vrf NetworkA 和 ping vrf NetworkA 192.168.2.9 source 192.168.1.1

26.3. 配置基本的 MPLS CE 路由器

提问 配置客户网络的边界路由器

回答

Router-CE-A1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-CE-A1(config)#**interface *FastEthernet0/0.1***

Router-CE-A1(config-if)#**encapsulation dot1Q *101***

Router-CE-A1(config-if)#**ip address *192.168.1.5 255.255.255.0***

Router-CE-A1(config-if)#**exit**

Router-CE-A1(config)#**ip route *0.0.0.0 0.0.0.0 192.168.1.1***

Router-CE-A1(config)# **exit**

Router-CE-A1#

注释 CE 路由器没有特殊的配置，只是需要到 MPLS 网络的路由而已，这里使用的是静态路由，使用其他动态路由协议也可以，这样两个不同的站点可以互通路由表

26.4. ATM 承载 MPLS

提问 配置运行于 ATM 网络上的 MPLS

回答

根据 ATM 交换机性能的不同大概有两种配置，一种是不参与 MPLS 只是基本的信元传递

Router-PE1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router-PE1(config)#**ip cef**

Router-PE1(config)#**mpls ip**

Router-PE1(config)#**interface *ATM1/0***

Router-PE1(config-if)#**no ip address**

Router-PE1(config-if)#**exit**

Router-PE1(config)#**interface *ATM1/0.1* mpls**

Router-PE1(config-if)#**ip address *10.1.1.2 255.255.255.252***

Router-PE1(config-if)#**mpls ip**

Router-PE1(config-if)#**exit**

Router-PE1(config)#**end**

Router-PE1#

Router-PE3#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-PE3(config)#**ip cef**

Router-PE3(config)#**mpls ip**

Router-PE3(config)#**interface *ATM1/0***

Router-PE3(config-if)#**no ip address**

Router-PE3(config-if)#**exit**

Router-PE3(config)#**interface *ATM1/0.1* mpls**

Router-PE3(config-if)#**ip address *10.1.1.1 255.255.255.252***

Router-PE3(config-if)#**mpls ip**

Router-PE3(config-if)#**exit**

Router-PE3(config)#**end**

Router-PE3#

ATM switch 交换机需要配置两个 PVCs: 一个用于控制 VC 一个用户数据 VC:

Switch-P2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Switch-P2(config)#**interface *ATM0/1/2***

Switch-P2(config-if)#**no ip address**

Switch-P2(config-if)#**exit**

Switch-P2(config)#**interface *ATM0/1/3***

Switch-P2(config-if)#**no ip address**

Switch-P2(config-if)#**atm pvc *0 32* interface *ATM0/1/2 0 32***

Switch-P2(config-if)#**atm pvc *1 33* interface *ATM0/1/2 1 33***

Switch-P2(config-if)#**exit**

Switch-P2(config)#**end**

Switch-P2#

另一种新的 ATM 交换机可以参与类似 P 路由器那样的 MPLS 包转发

Router-PE1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-PE1(config)#**ip cef**

Router-PE1(config)#**mpls ip**

Router-PE1(config)#**interface *ATM1/0***

Router-PE1(config-if)#**no ip address**

Router-PE1(config-if)#**exit**

Router-PE1(config)#**interface *ATM1/0.1* mpls**

Router-PE1(config-if)#**ip address *10.1.1.2 255.255.255.252***

Router-PE1(config-if)#**mpls ip**

Router-PE1(config-if)#**exit**

Router-PE1(config)#**end**

Router-PE1#

Router-PE3#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-PE3(config)#**ip cef**

Router-PE3(config)#**mpls ip**

Router-PE3(config)#**interface *ATM1/0***

Router-PE3(config-if)#**no ip address**

Router-PE3(config-if)#**exit**

Router-PE3(config)#**interface *ATM1/0.1* mpls**

Router-PE3(config-if)#**ip address *10.1.1.6 255.255.255.252***

Router-PE3(config-if)#**mpls ip**

Router-PE3(config-if)#**exit**

Router-PE3(config)#**end**

Router-PE3#

Switch-P2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Switch-P2(config)#**ip cef**

Switch-P2(config)#**mpls ip**

Switch-P2(config)#**interface *ATM0/1/2***

Switch-P2(config-if)#**ip address *10.1.1.5 255.255.255.252***

Switch-P2(config-if)#**mpls ip**

Switch-P2(config-if)#**exit**

Switch-P2(config)#**interface *ATM0/1/3***

Switch-P2(config-if)#**ip address *10.1.1.1 255.255.255.252***

Switch-P2(config-if)#**mpls ip**

Switch-P2(config-if)#**exit**

Switch-P2(config)#**interface *Loopback0***

Switch-P2(config-if)#**ip address *10.0.0.1 255.255.255.255***

Switch-P2(config-if)#**exit**

Switch-P2(config)#**router ospf *99***

Switch-P2(config-router)#**router-id *10.0.0.1***

Switch-P2(config-router)#**network *10.0.0.0 0.255.255.255* area *0***

Switch-P2(config-router)#**exit**

Switch-P2(config)#**end**

Switch-P2#

注释 注意这里的配置是不全的，只是和 ATM 有关的配置。第一种方式由于 VC 的配置所以扩展性不强，而另一种参与了 IGP 所以增强了扩展性

26.5. PE-CE 之间运行 RIP

提问 PE 和 CE 路由器之间启用 RIP 路由协议

回答

Router-CE-A2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-CE-A2(config)#**router rip**

Router-CE-A2(config-router)#**version *2***

Router-CE-A2(config-router)#**network *10.0.0.0***

Router-CE-A2(config-router)#**network *192.168.3.0***

```
Router-CE-A2(config-router)#end

Router-CE-A2#

Router-PE2#configure terminal

Enter configuration commands, one per line.    End with CNTL/Z.

Router-PE2(config)#router rip

Router-PE2(config-router)#version 2

Router-PE2(config-router)#address-family ipv4 vrf NetworkA

Router-PE2(config-router-af)#version 2

Router-PE2(config-router-af)#redistribute bgp 100 metric 4

Router-PE2(config-router-af)#network 192.168.3.0

Router-PE2(config-router-af)#exit-address-family

Router-PE2(config-router)#exit

Router-PE2(config)#router bgp 100

Router-PE2(config-router)#address-family ipv4 vrf NetworkA

Router-PE2(config-router-af)#redistribute rip metric 4

Router-PE2(config-router-af)#end

Router-PE2#
```

注释 这里需要注意的是 RIP 不是全局启用的，只是在特定的 VRF 下面的配置 address-family ipv4 vrf NetworkA，另外需要配置 RIP 和 MP-BGP 之间的路由再分布。这里的再分布和传统再分布不同的是，分布到 IGP 的路由不是标记为外部路由的

26.6. PE-CE 之间运行 OSPF

提问 PE 和 CE 路由器之间启用 OSPF 路由协议

回答

两个不同站点的 CE 路由器

Router-CE-A1#configure terminal

Enter configuration commands, one per line.   End with CNTL/Z.

Router-CE-A1(config)#**router ospf *55***

Router-CE-A1(config-router)#**network *192.168.1.0 0.0.0.255* area *0***

Router-CE-A1(config-router)#**network *192.168.5.0 0.0.0.255* area *0***

Router-CE-A1(config-router)#**end**

Router-CE-A1#

Router-CE-A2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-CE-A2(config)#**router ospf *55***

Router-CE-A2(config-router)#**network *192.168.3.0 0.0.0.255* area *0***

Router-CE-A2(config-router)#**end**

Router-CE-A2#

两个相应站点的 PE 路由器

Router-PE1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-PE1(config)#**router ospf *155* vrf *NetworkA***

Router-PE1(config-router)#**redistribute bgp *100* subnets**

Router-PE1(config-router)#**network *192.168.1.0 0.0.0.255* area *0***

Router-PE1(config-router)#**exit**

Router-PE1(config)#**router bgp** ***100***

Router-PE1(config-router)#**address-family ipv4 vrf** ***NetworkA***

Router-PE1(config-router-af)#**redistribute ospf** ***155***

Router-PE1(config-router-af)#**exit-address-family**

Router-PE1(config-router)#**end**

Router-PE1#

Router-PE2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-PE2(config)#**router ospf** ***155*** **vrf** ***NetworkA***

Router-PE2(config-router)#**redistribute bgp** ***100*** **subnets**

Router-PE2(config-router)#**network** ***192.168.3.0 0.0.0.255*** **area** ***0***

Router-PE2(config-router)#**exit**

Router-PE2(config)#**router bgp** ***100***

Router-PE2(config-router)#**address-family ipv4 vrf** ***NetworkA***

Router-PE2(config-router-af)#**redistribute ospf** ***155***

Router-PE2(config-router-af)#**exit-address-family**

Router-PE2(config-router)#**end**

Router-PE2#

注释 这里只是和路由相关的配置，其他配置略去。12.2(8)T 以后有 shamlink 这种特性来通过类似虚拟链路的方式修改 OSPF 的路由条目，从 inter-area 路由变为 intra-area 路由，

Router-PE1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-PE1(config)#**interface *Loopback155***

Router-PE1(config-if)#**ip vrf forwarding *NetworkA***

Router-PE1(config-if)#**ip address *192.168.155.1 255.255.255.255***

Router-PE1(config-if)#**exit**

Router-PE1(config)#**router ospf *155* vrf *NetworkA***

Router-PE1(config-router)#**area *0* sham-link *192.168.155.1 192.168.155.2* cost *10***

Router-PE1(config-router)#**redistribute bgp *100* subnets**

Router-PE1(config-router)#**network *192.168.1.0 0.0.0.255* area *0***

Router-PE1(config-router)#**end**

Router-PE1#

Router-PE2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-PE2(config)#**interface *Loopback155***

Router-PE2(config-if)#**ip vrf forwarding *NetworkA***

Router-PE2(config-if)#**ip address *192.168.155.2 255.255.255.255***

Router-PE2(config-if)#**exit**

Router-PE2(config)#**router ospf *155* vrf *NetworkA***

Router-PE2(config-router)#**area *0* sham-link *192.168.155.2 192.168.155.1* cost *10***

Router-PE2(config-router)#**redistribute bgp *100* subnets**

Router-PE2(config-router)#**network *192.168.3.0 0.0.0.255* area *0***

Router-PE2(config-router)#**end**

Router-PE2#

26.7. PE-CE 之间运行 EIGRP

提问 PE 和 CE 路由器之间启用 EIGRP 路由协议

回答

Router-CE-A1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router-CE-A1(config)#**router eigrp *156***

Router-CE-A1(config-router)#**network *192.168.1.0***

Router-CE-A1(config-router)#**network *192.168.5.0***

Router-CE-A1(config-router)#**no auto-summary**

Router-CE-A1(config-router)#**end**

Router-CE-A1#

Router-CE-A2#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router-CE-A2(config)#**router eigrp *156***

Router-CE-A2(config-router)#**network *10.0.0.0***

Router-CE-A2(config-router)#**network *192.168.3.0***

Router-CE-A2(config-router)#**no auto-summary**

Router-CE-A2(config-router)#**end**

Router-CE-A2#

Router-PE1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router-PE1(config)#**router eigrp *1001***

Router-PE1(config-router)#**no auto-summary**

Router-PE1(config-router)#**address-family ipv4 vrf *NetworkA***

Router-PE1(config-router-af)#**redistribute bgp *100* metric *10000 10 255 1 1500***

Router-PE1(config-router-af)#**network *192.168.1.0***

Router-PE1(config-router-af)#**no auto-summary**

Router-PE1(config-router-af)#**autonomous-system *156***

Router-PE1(config-router-af)#**exit-address-family**

Router-PE1(config-router)#**exit**

Router-PE1(config)#**router bgp *100***

Router-PE1(config-router)#**address-family ipv4 vrf *NetworkA***

Router-PE1(config-router-af)#**redistribute eigrp *156***

Router-PE1(config-router-af)#**exit-address-family**

Router-PE1(config-router)#**exit**

Router-PE1(config)#**end**

Router-PE1#

Router-PE2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-PE2(config)#**router eigrp *1001***

Router-PE2(config-router)#**auto-summary**

Router-PE2(config-router)#**address-family ipv4 vrf *NetworkA***

Router-PE2(config-router-af)#**redistribute bgp *100* metric *10000 10 255 1 1500***

Router-PE2(config-router-af)#**network *192.168.3.0***

Router-PE2(config-router-af)#**no auto-summary**

Router-PE2(config-router-af)#**autonomous-system *156***

Router-PE2(config-router-af)#**exit-address-family**

Router-PE2(config-router)#**end**

Router-PE2#

注释 注意的是 VRF 中自治域系统的配置和相应再分发所选择的 AS 配置，要确保 PE 和 CE 的一致，对 PE 这里有两个 EIGRP 的 AS 号

26.8. PE-CE 之间运行 BGP

提问 PE 和 CE 路由器之间启用 BGP 路由协议

回答

Router-CE-A1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router-CE-A1(config)#**router bgp *65535***

Router-CE-A1(config-router)#**neighbor *192.168.1.1* remote-as *100***

Router-CE-A1(config-router)#**redistribute ospf *155***

Router-CE-A1(config-router)#**no synchronization**

Router-CE-A1(config-router)#**no auto-summary**

Router-CE-A1(config-router)#**exit**

Router-CE-A1(config)#**router ospf *155***

Router-CE-A1(config-router)#**redistribute bgp *65535* subnets**

Router-CE-A1(config-router)#**network *192.168.5.0 0.0.0.255* area *0***

Router-CE-A1(config-router)#**end**

Router-CE-A1#

Router-CE-A2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-CE-A2(config)#**router bgp *65534***

Router-CE-A2(config-router)#**neighbor *192.168.3.1* remote-as *100***

Router-CE-A2(config-router)#**network *10.8.8.0* mask *255.255.255.0***

Router-CE-A2(config-router)#**network *192.168.3.0***

Router-CE-A2(config-router)#**no synchronization**

Router-CE-A2(config-router)#**no auto-summary**

Router-CE-A2(config-router)#**end**

Router-CE-A2#

Router-PE1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-PE1(config)#**router bgp *100***

Router-PE1(config-router)#**address-family ipv4 vrf *NetworkA***

Router-PE1(config-router-af)#**neighbor *192.168.1.5* remote-as *65535***

Router-PE1(config-router-af)#**neighbor *192.168.1.5* activate**

Router-PE1(config-router-af)#**end**

Router-PE1#

Router-PE2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-PE2(config)#**router bgp *100***

Router-PE2(config-router)#**address-family ipv4 vrf *NetworkA***

Router-PE2(config-router-af)#**neighbor *192.168.3.8* remote-as *65534***

Router-PE2(config-router-af)#**neighbor *192.168.3.8* activate**

Router-PE2(config-router-af)#**end**

Router-PE2#

注释 这里仍然不是全部的配置。对于 BGP 来说就不需要再配置再分布了，不过很少有运营商会支持客户网络的 BGP 互联

26.9. MPLS 上的 QOS

提问 配置 MPLS 上 QoS 的支持

回答

Router-PE1#**configure terminal**

Router-PE1(config)#**class-map match-any *med-priority***

Router-PE1(config-cmap)#**match precedence *1***

Router-PE1(config-cmap)#**match precedence *2***

Router-PE1(config-cmap)#**exit**

Router-PE1(config)#**class-map match-any *high-priority***

Router-PE1(config-cmap)#**match precedence *3***

Router-PE1(config-cmap)#**match precedence *4***

Router-PE1(config-cmap)#**match precedence *5***

Router-PE1(config-cmap)#**exit**

Router-PE1(config)#**class-map match-any *realtime-priority***

Router-PE1(config-cmap)#**match precedence *6***

Router-PE1(config-cmap)#**match dscp *ef***

Router-PE1(config-cmap)#**exit**

Router-PE1(config)#**policy-map *MPLS-priority***

Router-PE1(config-pmap)#**class *realtime-priority***

Router-PE1(config-pmap-c)#**priority percent *10***

Router-PE1(config-pmap-c)#**set mpls experimental topmost *3***

Router-PE1(config-pmap-c)#**exit**

Router-PE1(config-pmap)#**class *high-priority***

Router-PE1(config-pmap-c)#**bandwidth percent *10***

Router-PE1(config-pmap-c)#**queue-limit *20***

Router-PE1(config-pmap-c)#**set mpls experimental topmost *2***

Router-PE1(config-pmap-c)#**exit**

Router-PE1(config-pmap)#**class *med-priority***

Router-PE1(config-pmap-c)#**bandwidth percent *15***

Router-PE1(config-pmap-c)#**queue-limit *50***

Router-PE1(config-pmap-c)#**set mpls experimental topmost *1***

Router-PE1(config-pmap-c)#**exit**

Router-PE1(config-pmap)#**class *class-default***

Router-PE1(config-pmap-c)#**bandwidth percent *40***

Router-PE1(config-pmap-c)#**random-detect**

Router-PE1(config-pmap-c)#**set mpls experimental topmost *0***

Router-PE1(config-pmap-c)#**exit**

Router-PE1(config-pmap)#**exit**

Router-PE1(config)#**interface *Serial0/0***

Router-PE1(config-if)#**service-policy output *MPLS-priority***

Router-PE1(config-if)#**exit**

Router-PE1(config)#**end**

Router-PE1#

Router-P1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-P1(config)#**class-map match-any *med-priority***

Router-P1(config-cmap)#**match mpls experimental topmost *1***

Router-P1(config-cmap)#**exit**

Router-P1(config)#**class-map match-any *high-priority***

Router-P1(config-cmap)#**match mpls experimental topmost *2***

Router-P1(config-cmap)#**exit**

Router-P1(config)#**class-map match-any *realtime-priority***

Router-P1(config-cmap)#**match mpls experimental topmost *3***

Router-P1(config-cmap)#**exit**

Router-P1(config)#**policy-map *MPLS-priority***

Router-P1(config-pmap)#**class *realtime-priority***

Router-P1(config-pmap-c)#**priority percent *10***

Router-P1(config-pmap-c)#**exit**

Router-P1(config-pmap)#**class *high-priority***

Router-P1(config-pmap-c)#**bandwidth percent *10***

Router-P1(config-pmap-c)#**queue-limit *20***

Router-P1(config-pmap-c)#**exit**

Router-P1(config-pmap)#**class *med-priority***

Router-P1(config-pmap-c)#**bandwidth percent *15***

Router-P1(config-pmap-c)#**queue-limit *50***

Router-P1(config-pmap-c)#**exit**

Router-P1(config-pmap)#**class *class-default***

Router-P1(config-pmap-c)#**bandwidth percent *40***

Router-P1(config-pmap-c)#**random-detect**

Router-P1(config-pmap-c)#**exit**

Router-P1(config-pmap)#**exit**

Router-P1(config)#**interface *FastEthernet0/0***

Router-P1(config-if)#**service-policy output *MPLS-priority***

Router-P1(config-if)#**exit**

Router-P1(config)#**end**

Router-P1#

注释 简单的说就是 PE 做客户网络数据包的 DSCP 或者 IP 优先级位和 MPLS EXP 优先级位之间的转化，EXP 目前只能支持四种类型的数据包。很有用的验证命令

Router-P1#**show policy interface *FastEthernet0/0***

FastEthernet0/0

```
Service-policy output: MPLS-priority


  Class-map: realtime-priority (match-any)

    0 packets, 0 bytes

    5 minute offered rate 0 bps, drop rate 0 bps

    Match: mpls experimental topmost 3

      0 packets, 0 bytes

      5 minute rate 0 bps

    Queueing

      Strict Priority

      Output Queue: Conversation 264

      Bandwidth 10 (%)

      Bandwidth 10000 (kbps) Burst 250000 (Bytes)

      (pkts matched/bytes matched) 0/0

      (total drops/bytes drops) 0/0
```

26.10. AUTOROUTE 和 MPLS 流量工程

提问 使用 autoroute 特性来自动维护 MPLS 网络的流量工程路径

回答

Router-PE1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router-PE1(config)#**mpls traffic-eng tunnels**

Router-PE1(config)#**interface *Loopback0***

Router-PE1(config-if)#**ip address *10.0.0.2 255.255.255.255***

Router-PE1(config-if)#**exit**

Router-PE1(config)#**interface *Tunnel11***

Router-PE1(config-if)#**ip unnumbered *Loopback0***

Router-PE1(config-if)#**tunnel destination *10.0.0.3***

Router-PE1(config-if)#**tunnel mode mpls traffic-eng**

Router-PE1(config-if)#**tunnel mpls traffic-eng autoroute announce**

Router-PE1(config-if)#**tunnel mpls traffic-eng priority *7 7***

Router-PE1(config-if)#**tunnel mpls traffic-eng bandwidth *256***

Router-PE1(config-if)#**tunnel mpls traffic-eng path-option *1* explicit name *def-PE3***

Router-PE1(config-if)#**exit**

Router-PE1(config)#**interface *Tunnel12***

Router-PE1(config-if)#**ip unnumbered *Loopback0***

Router-PE1(config-if)#**tunnel destination *10.0.0.3***

Router-PE1(config-if)#**tunnel mode mpls traffic-eng**

Router-PE1(config-if)#**tunnel mpls traffic-eng autoroute announce**

Router-PE1(config-if)#**tunnel mpls traffic-eng priority *7 7***

Router-PE1(config-if)#**tunnel mpls traffic-eng bandwidth *256***

Router-PE1(config-if)#**tunnel mpls traffic-eng path-option *1* explicit name *hi-PE3***

Router-PE1(config-if)#**exit**

Router-PE1(config)#**interface *Serial0/0***

Router-PE1(config-if)#**ip address *10.1.1.13 255.255.255.252***

Router-PE1(config-if)#**mpls traffic-eng tunnels**

Router-PE1(config-if)#**tag-switching ip**

Router-PE1(config-if)#**ip rsvp bandwidth *512***

Router-PE1(config-if)#**exit**

Router-PE1(config)#**interface *ATM1/0.1* tag-switching**

Router-PE1(config-subif)#**ip address *10.1.1.2 255.255.255.252***

Router-PE1(config-subif)#**mpls traffic-eng tunnels**

Router-PE1(config-subif)#**tag-switching ip**

Router-PE1(config-subif)#**ip rsvp bandwidth *4000***

Router-PE1(config-subif)#**exit**

Router-PE1(config)#**router ospf *99***

Router-PE1(config-router)#**router-id *10.0.0.2***

Router-PE1(config-router)#**log-adjacency-changes**

Router-PE1(config-router)#**network *10.0.0.0 0.255.255.255* area *0***

Router-PE1(config-router)#**mpls traffic-eng router-id *Loopback0***

Router-PE1(config-router)#**mpls traffic-eng area *0***

Router-PE1(config-router)#**exit**

Router-PE1(config)#**ip explicit-path name *def-PE3* enable**

Router-PE1(cfg-ip-expl-path)#**next-address *10.1.1.14***

Explicit Path name def-PE3:

1: next-address 10.1.1.14

Router-PE1(cfg-ip-expl-path)#**next-address** ***10.1.1.9***

Explicit Path name def-PE3:

    1: next-address 10.1.1.14

    2: next-address 10.1.1.9

Router-PE1(cfg-ip-expl-path)#**exit**

Router-PE1(config)#**ip explicit-path name** ***hi-PE3*** **enable**

Router-PE1(cfg-ip-expl-path)#**next-address** ***10.1.1.1***

Explicit Path name hi-PE3:

    1: next-address 10.1.1.1

Router-PE1(cfg-ip-expl-path)#**next-address** ***10.1.1.6***

Explicit Path name hi-PE3:

    1: next-address 10.1.1.1

    2: next-address 10.1.1.6

Router-PE1(cfg-ip-expl-path)#**exit**

Router-PE1(config)#**end**

Router-PE1#

Router-PE3#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-PE3(config)#**mpls traffic-eng tunnels**

Router-PE3(config)#**interface** ***Loopback0***

Router-PE3(config-if)#**ip address** ***10.0.0.3 255.255.255.255***

Router-PE3(config-if)#**exit**

Router-PE3(config)#**interface *Tunnel11***

Router-PE3(config-if)#**ip unnumbered *Loopback0***

Router-PE3(config-if)#**tunnel destination *10.0.0.2***

Router-PE3(config-if)#**tunnel mode mpls traffic-eng**

Router-PE3(config-if)#**tunnel mpls traffic-eng autoroute announce**

Router-PE3(config-if)#**tunnel mpls traffic-eng priority *7 7***

Router-PE3(config-if)#**tunnel mpls traffic-eng bandwidth *256***

Router-PE3(config-if)#**tunnel mpls traffic-eng path-option *1* explicit name *def-PE1***

Router-PE3(config-if)#**exit**

Router-PE3(config)#**interface *Tunnel12***

Router-PE3(config-if)#**ip unnumbered *Loopback0***

Router-PE3(config-if)#**tunnel destination *10.0.0.2***

Router-PE3(config-if)#**tunnel mode mpls traffic-eng**

Router-PE3(config-if)#**tunnel mpls traffic-eng autoroute announce**

Router-PE3(config-if)#**tunnel mpls traffic-eng priority *7 7***

Router-PE3(config-if)#**tunnel mpls traffic-eng bandwidth *256***

Router-PE3(config-if)#**tunnel mpls traffic-eng path-option *1* explicit name *hi-PE1***

Router-PE3(config-if)#**exit**

Router-PE3(config)#**interface *Serial0/0***

Router-PE3(config-if)#**ip address *10.1.1.9 255.255.255.252***

Router-PE3(config-if)#**mpls traffic-eng tunnels**

Router-PE3(config-if)#**tag-switching ip**

Router-PE3(config-if)#**ip rsvp bandwidth *512***

Router-PE3(config-if)#**exit**

Router-PE3(config)#**interface *ATM1/0.1* tag-switching**

Router-PE3(config-subif)#**ip address *10.1.1.6 255.255.255.252***

Router-PE3(config-subif)#**mpls traffic-eng tunnels**

Router-PE3(config-subif)#**tag-switching ip**

Router-PE3(config-subif)#**ip rsvp bandwidth *4000***

Router-PE3(config-subif)#**exit**

Router-PE3(config)#**router ospf *99***

Router-PE3(config-router)#**router-id *10.0.0.3***

Router-PE3(config-router)#**log-adjacency-changes**

Router-PE3(config-router)#**network *10.0.0.0 0.255.255.255* area *0***

Router-PE3(config-router)#**mpls traffic-eng router-id *Loopback0***

Router-PE3(config-router)#**mpls traffic-eng area *0***

Router-PE3(config-router)#**exit**

Router-PE3(config)#**ip explicit-path name *def-PE1* enable**

Router-PE3(cfg-ip-expl-path)#**next-address *10.1.1.10***

Explicit Path name def-PE1:

    1: next-address 10.1.1.10

Router-PE3(cfg-ip-expl-path)#**next-address *10.1.1.13***

Explicit Path name def-PE1:

    1: next-address 10.1.1.10

2: next-address 10.1.1.13

Router-PE3(cfg-ip-expl-path)#**exit**

Router-PE3(config)#**ip explicit-path name *hi-PE1* enable**

Router-PE3(cfg-ip-expl-path)#**next-address *10.1.1.5***

Explicit Path name hi-PE1:

1: next-address 10.1.1.5

Router-PE3(cfg-ip-expl-path)#**next-address *10.1.1.2***

Explicit Path name hi-PE1:

1: next-address 10.1.1.5

2: next-address 10.1.1.2

Router-PE3(cfg-ip-expl-path)#**exit**

Router-PE3(config)#**end**

Router-PE3#

Router-P1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router-P1(config)#**mpls traffic-eng tunnels**

Router-P1(config)#**interface *Loopback0***

Router-P1(config-if)#**ip address *10.0.0.11 255.255.255.255***

Router-P1(config-if)#**exit**

Router-P1(config)#**interface *Serial0/0***

Router-P1(config-if)#**ip address *10.1.1.14 255.255.255.252***

Router-P1(config-if)#**tag-switching ip**

Router-P1(config-if)#**mpls traffic-eng tunnels**

Router-P1(config-if)#**ip rsvp bandwidth *512***

Router-P1(config-if)#**exit**

Router-P1(config)#**interface *Serial0/1***

Router-P1(config-if)#**ip address *10.1.1.10 255.255.255.252***

Router-P1(config-if)#**tag-switching ip**

Router-P1(config-if)#**mpls traffic-eng tunnels**

Router-P1(config-if)#**ip rsvp bandwidth *512***

Router-P1(config-if)#**exit**

Router-P1(config)#**router ospf *99***

Router-P1(config-router)#**router-id *10.0.0.11***

Router-P1(config-router)#**log-adjacency-changes**

Router-P1(config-router)#**network *10.0.0.0 0.255.255.255* area *0***

Router-P1(config-router)#**mpls traffic-eng router-id *Loopback0***

Router-P1(config-router)#**mpls traffic-eng area *0***

Router-P1(config-router)#**exit**

Router-P1(config)#**end**

Router-P1#

注释 很复杂啊，还没很明白

26.11. MPLS 上的组播

提问 配置 MPLS 网络对客户组播的支持

回答

Router-C-An#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-C-An(config)#**ip multicast-routing**

Router-C-An(config)#**interface *FastEthernet0/0***

Router-C-An(config-if)#**ip address *192.168.5.12 255.255.255.0***

Router-C-An(config-if)#**ip pim sparse-dense-mode**

Router-C-An(config-if)#**exit**

Router-C-An(config)#**end**

Router-C-An#

Router-CE-A1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-CE-A1(config)#**ip multicast-routing**

Router-CE-A1(config)#**interface *FastEthernet0/0.1***

Router-CE-A1(config-subif)#**encapsulation dot1Q *101***

Router-CE-A1(config-subif)#**ip address *192.168.1.5 255.255.255.0***

Router-CE-A1(config-subif)#**ip pim sparse-dense-mode**

Router-CE-A1(config-subif)#**exit**

Router-CE-A1(config)#**interface *FastEthernet0/0.2***

Router-CE-A1(config-subif)#**encapsulation dot1Q *111***

Router-CE-A1(config-subif)#**ip address *192.168.5.1 255.255.255.0***

Router-CE-A1(config-subif)#**ip pim sparse-dense-mode**

```
Router-CE-A1(config-subif)#exit
Router-CE-A1(config)#end
Router-CE-A1#
Router-CE-A2#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router-CE-A2(config)#ip multicast-routing
Router-CE-A2(config)#interface Loopback0
Router-CE-A2(config-if)#ip address 10.8.8.8 255.255.255.255
Router-CE-A2(config-if)#ip pim sparse-dense-mode
Router-CE-A2(config-if)#ip igmp join-group 239.1.1.1
Router-CE-A2(config-if)#exit
Router-CE-A2(config)#interface Ethernet0
Router-CE-A2(config-if)#ip address 192.168.3.8 255.255.255.0
Router-CE-A2(config-if)#ip pim sparse-dense-mode
Router-CE-A2(config-if)#exit
Router-CE-A2(config)#end
Router-CE-A2#
Router-PE1#configure terminal
Enter configuration commands, one per line.    End with CNTL/Z.
Router-PE1(config)#ip multicast-routing
Router-PE1(config)#interface Loopback0
Router-PE1(config-if)#ip address 10.0.0.2 255.255.255.255
```

Router-PE1(config-if)#**ip pim sparse-dense-mode**

Router-PE1(config-if)#**exit**

Router-PE1(config)#**interface *Serial0/0***

Router-PE1(config-if)#**ip address *10.1.1.13 255.255.255.252***

Router-PE1(config-if)#**ip pim sparse-dense-mode**

Router-PE1(config-if)#**tag-switching ip**

Router-PE1(config-if)#**exit**

Router-PE1(config)#**ip multicast-routing vrf *NetworkA***

Router-PE1(config)#**ip vrf *NetworkA***

Router-PE1(config-vrf)#**rd *100:1***

Router-PE1(config-vrf)#**route-target export *100:1***

Router-PE1(config-vrf)#**route-target import *100:1***

Router-PE1(config-vrf)#**mdt default *239.100.100.1***

Router-PE1(config-vrf)#**exit**

Router-PE1(config)#**interface *Loopback155***

Router-PE1(config-if)#**ip vrf forwarding *NetworkA***

Router-PE1(config-if)#**ip address *192.168.155.1 255.255.255.255***

Router-PE1(config-if)#**ip pim sparse-dense-mode**

Router-PE1(config-if)#**exit**

Router-PE1(config)#**interface *Ethernet0/0***

Router-PE1(config-if)#**description *connection to customer A, site 1***

Router-PE1(config-if)#**ip vrf forwarding *NetworkA***

Router-PE1(config-if)#**ip address *192.168.1.1 255.255.255.0***

Router-PE1(config-if)#**ip pim sparse-dense-mode**

Router-PE1(config-if)#**exit**

Router-PE1(config)#**ip pim vrf *NetworkA* send-rp-announce *Loopback155* scope *15***

Router-PE1(config)#**ip pim vrf *NetworkA* send-rp-discovery *Loopback155* scope *15***

Router-PE1(config)#**end**

Router-PE1#

Router-PE2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-PE2(config)#**ip multicast-routing**

Router-PE2(config)#**interface *Loopback0***

Router-PE2(config-if)#**ip address *10.0.0.4 255.255.255.255***

Router-PE2(config-if)#**ip pim sparse-dense-mode**

Router-PE2(config-if)#**exit**

Router-PE2(config)#**interface *FastEthernet0/0.1***

Router-PE2(config-subif)#**encapsulation dot1Q *10***

Router-PE2(config-subif)#**ip address *10.1.2.4 255.255.255.0***

Router-PE2(config-subif)#**ip pim sparse-dense-mode**

Router-PE2(config-subif)#**tag-switching ip**

Router-PE2(config-subif)#**exit**

Router-PE2(config)#**ip multicast-routing vrf *NetworkA***

Router-PE2(config)#**ip vrf *NetworkA***

Router-PE2(config-vrf)#**rd *100:1***

Router-PE2(config-vrf)#**route-target export *100:1***

Router-PE2(config-vrf)#**route-target import *100:1***

Router-PE2(config-vrf)#**mdt default *239.100.100.1***

Router-PE2(config-vrf)#**exit**

Router-PE2(config)#**interface *Loopback155***

Router-PE2(config-if)#**ip vrf forwarding *NetworkA***

Router-PE2(config-if)#**ip address *192.168.155.2 255.255.255.255***

Router-PE2(config-if)#**ip pim sparse-dense-mode**

Router-PE2(config-if)#**exit**

Router-PE2(config)#**interface *FastEthernet0/0.2***

Router-PE2(config-subif)#**encapsulation dot1Q *102***

Router-PE2(config-subif)#**ip vrf forwarding *NetworkA***

Router-PE2(config-subif)#**ip address *192.168.3.1 255.255.255.0***

Router-PE2(config-subif)#**ip pim sparse-dense-mode**

Router-PE2(config-subif)#**exit**

Router-PE2(config)#**end**

Router-PE2#

Router-P1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-P1(config)#**ip multicast-routing**

Router-P1(config)#**interface *FastEthernet0/0***

Router-P1(config-if)#**ip address *10.1.2.11 255.255.255.0***

Router-P1(config-if)#**ip pim sparse-dense-mode**

Router-P1(config-if)#**tag-switching ip**

Router-P1(config-if)#**exit**

Router-P1(config)#**interface *Serial0/0***

Router-P1(config-if)#**ip address *10.1.1.14 255.255.255.252***

Router-P1(config-if)#**ip pim sparse-dense-mode**

Router-P1(config-if)#**tag-switching ip**

Router-P1(config-if)#**exit**

Router-P1(config)#**interface *Serial0/1***

Router-P1(config-if)#**ip address *10.1.1.10 255.255.255.252***

Router-P1(config-if)#**ip pim sparse-dense-mode**

Router-P1(config-if)#**tag-switching ip**

Router-P1(config-if)#**exit**

Router-P1(config)#**end**

Router-P1#

注释 无

26.12. 服务商不能我能

提问 通过其他方式来实现运营商所不能提供的特性

回答

Router-CE-A1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-CE-A1(config)#**ip multicast-routing**

Router-CE-A1(config)#**interface *FastEthernet0/0.1***

Router-CE-A1(config-if)#**encapsulation dot1Q *101***

Router-CE-A1(config-if)#**ip address *192.168.1.5 255.255.255.0***

Router-CE-A1(config-if)#**exit**

Router-CE-A1(config)#**interface Loopback*1***

Router-CE-A1(config-if)#**ip address *192.168.101.1 255.255.255.255***

Router-CE-A1(config-if)#**exit**

Router-CE-A1(config)#**interface Tunnel*1***

Router-CE-A1(config-if)#**ip address *192.168.152.1 255.255.255.252***

Router-CE-A1(config-if)#**tunnel source *192.168.101.1***

Router-CE-A1(config-if)#**tunnel destination *192.168.101.2***

Router-CE-A1(config-if)#**ip pim sparse-dense-mode**

Router-CE-A1(config-if)#**exit**

Router-CE-A1(config)#**router bgp *65535***

Router-CE-A1(config-router)#**neighbor *192.168.1.1* remote-as *100***

Router-CE-A1(config-router)#**network *192.168.1.0***

Router-CE-A1(config-router)#**network *192.168.101.1 mask 255.255.255.255***

Router-CE-A1(config-router)#**no synchronization**

Router-CE-A1(config-router)#**no auto-summary**

Router-CE-A1(config-router)#**exit**

Router-CE-A1(config)#**router ospf *155***

Router-CE-A1(config-router)#**network *192.168.5.0 0.0.0.255* area *0***

Router-CE-A1(config-router)#**network *192.168.152.0 0.0.0.255* area *0***

Router-CE-A1(config-router)#**exit**

Router-CE-A1(config)#**end**

Router-CE-A1#

Router-CE-A2#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router-CE-A2(config)#**ip multicast-routing**

Router-CE-A2(config)#**interface *Ethernet0***

Router-CE-A2(config-if)#**ip address *192.168.3.8 255.255.255.0***

Router-CE-A2(config-if)#**exit**

Router-CE-A2(config)#**interface Loopback*1***

Router-CE-A2(config-if)#**ip address *192.168.101.2 255.255.255.255***

Router-CE-A2(config-if)#**exit**

Router-CE-A2(config)#**interface Tunnel*1***

Router-CE-A2(config-if)#**ip address *192.168.152.2 255.255.255.252***

Router-CE-A2(config-if)#**tunnel source *192.168.101.2***

Router-CE-A2(config-if)#**tunnel destination *192.168.101.1***

Router-CE-A2(config-if)#**ip pim sparse-dense-mode**

Router-CE-A2(config-if)#**exit**

Router-CE-A2(config)#**router bgp *65534***

Router-CE-A2(config-router)#**neighbor *192.168.3.1* remote-as *100***

Router-CE-A2(config-router)#**network *192.168.3.0***

Router-CE-A2(config-router)#**network *192.168.101.2* mask *255.255.255.0***

Router-CE-A2(config-router)#**no synchronization**

Router-CE-A2(config-router)#**no auto-summary**

Router-CE-A2(config-router)#**exit**

Router-CE-A2(config)#**router ospf *155***

Router-CE-A2(config-router)#**network *10.8.8.0 0.0.0.255* area *0***

Router-CE-A2(config-router)#**network *192.168.152.0 0.0.0.255* area *0***

Router-CE-A2(config-router)#**exit**

Router-CE-A2(config)#**end**

Router-CE-A2#

注释 这里只是 CE 的配置，PE 配置参考 26.8。这里在服务商只支持 BGP 互联的网络中实现了 OSPF 和组播的传递

第二十七章 安全

27.1. 使用 AUTOSECURE

提问 傻瓜化的方式来加固你的路由器

回答

Router2#**auto secure**

--- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of

the router, but it will not make it absolutely resistant

to all security attacks ***

AutoSecure will modify the configuration of your device.

All configuration changes will be shown. For a detailed

explanation of how the configuration changes enhance security

and any possible side effects, please refer to Cisco.com for

Autosecure documentation.

At any prompt you may enter '?' for help.

Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]:

<Removed for brevity>

注释 12.3(1)开始路由器增加了 autosecure 的特性来通过问题的方式自动对路由器进行加固，下面是一个生成的配置实例

Router2#**show auto secure config**

no service finger

no service pad

no service udp-small-servers

no service tcp-small-servers

```
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no snmp-server community public
no snmp-server community private
banner ^C   Test ^C
security passwords min-length 6
security authentication failure rate 10 log
enable password 7 00071A1507545B54
aaa new-model
aaa authentication login local_auth local
line con 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
```

```
  login authentication local_auth
  exec-timeout 10 0
  transport output telnet
line vty 0 6
  login authentication local_auth
  transport input telnet
login block-for 5 attempts 5 within 6


crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 6
  transport input ssh telnet
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/0
  no ip redirects
```

```
  no ip proxy-arp
  no ip unreachables
  no ip directed-broadcast
  no ip mask-reply
!
interface Serial0/0
  no ip redirects
  no ip proxy-arp
  no ip unreachables
  no ip directed-broadcast
  no ip mask-reply
!
ip cef
Router2#
```


27.2. 使用基于上下文的控制列表（CONTEXT-BASED ACCESS-LISTS）

提问 配置路由器类似防火墙的高级过滤功能

回答

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**access-list 166 deny   ip any any**

Router1(config)#**access-list 167 permit tcp any any eq telnet**

Router1(config)#**ip inspect name *Telnet* tcp**

Router1(config)#**interface *Serial0/1***

Router1(config-if)#**ip access-group 166 in**

Router1(config-if)#**ip access-group 167 out**

Router1(config-if)#**ip inspect *Telnet* out**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 必须安装了支持 IOS 防火墙特性集的 IOS 才可以有此功能。CBAC 提供了类似防火墙的状态检查功能，可以动态的生成控制列表来允许回程的数据包，对于上述例子，回来的 telnet 数据包可以允许通过

Router1#**show ip inspect sessions**

Established Sessions

Session 821061C0 (172.25.1.1:1379)=>(10.2.2.2:23) tcp SIS_OPEN

Router1#

对于以前提到的被动 FTP 访问问题，也可以采用下面方法安全解决

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**access-list 155 permit tcp any any eq ftp**

Router1(config)#**access-list 155 deny ip any any**

Router1(config)#**ip inspect name *TEST* ftp**

Router1(config)#**interface *Serial0/0***

Router1(config-subif)#**ip access-group 155 in**

Router1(config-subif)#**ip inspect *TEST* in**

Router1(config-subif)#**exit**

Router1(config)#**end**

Router1#

Router1#**show ip access-list 155**

Extended IP access list 155

permit **tcp host 172.20.1.2 eq 11252 host 172.25.1.3 eq 49155 (1415 matches)**

permit tcp any any eq ftp (151 matches)

deny ip any any (3829 matches)

Router1#

同时也提供了对不同的会话的定时器配置

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip inspect tcp idle-time *1800***

Router1(config)#**ip inspect udp idle-time *20***

Router1(config)#**ip inspect tcp finwait-time *1***

Router1(config)#**ip inspect tcp synwait-time *15***

Router1(config)#**end**

Router1#

通过 show ip inspect config 命令来显示当前 CBAC 的配置

也增加了对 log 的支持 **ip inspect name *Telnet* tcp audit-trail on**

27.3. 透明 IOS 防火墙

提问 配置路由器作为 2 层防火墙

回答

首先配置 Integrated Routing and Bridging (IRB)的支持

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**bridge *1* protocol ieee**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**bridge-group *1***

Router1(config-if)#**interface *FastEthernet0/1***

Router1(config-if)#**bridge-group *1***

Router1(config-if)#**exit**

Router1(config)#**bridge irb**

Router1(config)#**bridge *1* route ip**

Router1(config)#**interface *BVI1***

Router1(config-if)#**ip address *172.25.1.101 255.255.255.0***

Router1(config-if)#**no shutdown**

Router1(config-if)#**end**

Router1#

然后配置防火墙的检查规则和 ACL

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**ip inspect name *OREILLY* tcp**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip inspect *OREILLY* in**

Router1(config-if)#**exit**

Router1(config)#**access-list *111* deny tcp any host *172.25.1.102* eq *23***

Router1(config)#**access-list *111* permit ip any any**

Router1(config)#**access-list *112* deny ip any any**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip access-group *111* in**

Router1(config-if)#**interface *FastEthernet0/1***

Router1(config-if)#**ip access-group *112* in**

Router1(config-if)#**end**

Router1#

注释 从 12.3(7)T 开始支持这种 2 层防火墙或者说透明防火墙的支持，这样可以透明于网络不需要做地址的更改，采用了 CBAC 的方式来过滤

27.4. 防止拒绝服务攻击

提问 通过对半开放连接的限制来防范拒绝服务攻击

回答

Router1#configure terminal

Router1(config)#**access-list *109* permit ip any host *192.168.99.2***

Router1(config)#**ip tcp intercept list *109***

Router1(config)#**ip tcp intercept max-incomplete high *10***

Router1(config)#**ip tcp intercept one-minute high *15***

Router1(config)#**ip tcp intercept max-incomplete low *5***

Router1(config)#**ip tcp intercept one-minute low *10***

Router1(config)#**end**

Router1#

注释 除了上述的配置以外还可以对丢弃模式等进行控制

Router1(config)#**ip tcp intercept drop-mode random**

Router1(config)#**ip tcp intercept watch-timeout *15***

Router1(config)#**ip tcp intercept mode watch**

比较有用的一个统计命令

Router1#**show tcp intercept statistics**

Intercepting new connections using access-list 109

9 incomplete, 1 established connections (total 10)

8 connection requests per minute

Router1#

27.5. 在非标准端口检查应用

提问 检查非标准端口的应用

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**ip port-map http port tcp *8000***

Router1(config)#**end**

Router1#

注释 也可以将 PAM 应用于特定的地址

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**access-list *22* permit host *10.1.2.14***

Router1(config)#**ip port-map http port *8080* list *22***

Router1(config)#**end**

Router1#

Router1#**show ip port-map http**

Default mapping: http tcp port 80 system defined

Default mapping: http tcp port 8000 user defined

Host specific: http tcp port 8080 in list 22 user defined

27.6. 入侵监测和预防

提问 利用内置的入侵监测软件来防范攻击

回答

12.3(8)T 之前叫 IDS

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**access-list *21* deny *192.168.100.205***

Router1(config)#**access-list *21* permit any**

Router1(config)#**ip audit notify log**

Router1(config)#**ip audit info action alarm drop reset**

Router1(config)#**ip audit attack action alarm drop reset**

Router1(config)#**ip audit smtp spam *10***

Router1(config)#**ip audit signature 1107 disable**

Router1(config)#**ip audit signature 2004 disable**

Router1(config)#**ip audit name *COOKBOOK* info list *21* action alarm drop reset**

Router1(config)#**ip audit name *COOKBOOK* attack list *21* action alarm drop reset**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip audit *COOKBOOK* in**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

以后叫 IPS

Router1#**configure terminal**

Enter configuration commands, one per line.   End with CNTL/Z.

Router1(config)#**access-list *21* deny *192.168.100.205***

Router1(config)#**access-list *21* permit any**

Router1(config)#**ip ips name *NEOSHI* list *21***

Router1(config)#**ip ips signature *4050* disable**

Router1(config)#**ip ips fail closed**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip ips *NEOSHI* in**

Router1(config-if)#**exit**

Router1(config)#**end**

Router1#

注释 Router1#**show ip ips statistics**

Signature statistics [process switch:fast switch]

signature 4050:0 packets checked: [**0:85**]

Interfaces configured for ips 1

Session creations since subsystem startup or last reset 0

Current session counts (estab/half-open/terminating) [0:0:0]

Maxever session counts (estab/half-open/terminating) [0:0:0]

Last session created never

Last statistic reset never

27.7. 登录密码重试锁定

提问 防止对登录密码的暴力破解

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**username *kwiley* password *test123***

Router1(config)#**aaa new-model**

Router1(config)#**aaa authentication login local_auth local**

Router1(config)#**aaa local authentication attempts max-fail *6***

Router1(config)#**line vty 0 4**

Router1(config-line)#**login authentication local_auth**

Router1(config-line)#**end**

Router1#

注释 12.3(14)T 以后开始可以限制对登录密码的尝试限定，解除锁定使用 Router1#**clear aaa local user lockout username *kwiley*** 当然要防止黑客利用此特性对合法用户名进行故意的锁定攻击

27.8. 认证代理（AUTHENTICATION PROXY）

提问 对单个用户进行认证和授权的访问控制

回答

Router1#**configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

Router1(config)#**aaa new-model**

Router1(config)#**aaa authorization auth-proxy default local**

Router1(config)#**ip auth-proxy auth-proxy-banner http**

Router1(config)#**ip auth-proxy name *HTTPPROXY* http**

Router1(config)#**ip admission auth-proxy-banner http**

Router1(config)#**interface *FastEthernet0/0***

Router1(config-if)#**ip auth-proxy *HTTPPROXY***

Router1(config-if)#**ip http server**

Router1(config)#**ip http authentication local**

Router1(config)#**end**

Router1#

注释 此认证代理可以截取用户的访问请求，然后用户可以在任何地方输入认证信息后访问，查看当前的认证缓存

Router1#**show ip auth-proxy cache**

Authentication Proxy Cache

Client Name ijbrown, Client IP 172.25.1.52, Port 4224, timeout 60, Time Remaining 53, state ESTAB